

Good Mobile Defense™

User's Guide

Version 3.8.5

Copyright, trademark and patent information.

©Good Technology, Inc. 2001-2006. All rights reserved. All use subject to license terms posted at www.good.com/legaldocs. Good, Good Technology, the Good logo, Good Mobile Messaging, Good Mobile Intranet, GoodInfo, GoodAccess, GoodControl, GoodLink Forms, GoodLink and powered by Good are trademarks of Good Technology, Inc. VeriSign(R) is a registered trademark of VeriSign, Inc. All other trademarks and service marks contained herein are the property of their respective owners. For example, Microsoft, Windows, Windows NT, Exchange and Outlook are trademarks of Microsoft Corporation. RIM, Research in Motion, RIM 950, RIM 957, and BlackBerry are registered trademarks or trademarks of Research in Motion Limited. Mobitex is a trademark of the Swedish Telecommunications Administration that may be registered in some jurisdictions. Datalight is a registered trademark of Datalight, Inc. FlashFX(tm) is a trademark of Datalight, Inc. Cingular, Cingular Wireless, the Cingular Icon, Xpress Mail, and Xpress Mail with GoodLink are trademarks of Cingular Wireless, LLC. All rights reserved.

Some or all of the following notices may apply to portions of the software or documentation provided by Good Technology, Inc.: Outside In@Wireless Export © 2001 Stellant Chicago, Inc. All rights reserved. Copyright 1993-2001 Datalight, Inc., All Rights Reserved. U.S. Patent Office 5,860,082. Code written by John Halleck is used with his permission. This distribution contains executables of the Netscape® Security Service (NSS) and Netscape Portable Runtime (NSPR). You may obtain the source code for these files from www.mozilla.org, which source files are subject to the Mozilla Public License 1.1. Part of the software embedded in this product is eCos - Embedded Configurable Operating System, a trademark of Red Hat. Portions created by Red Hat are Copyright (C) 1998, 1999, 2000 Red Hat, Inc. (<http://www.redhat.com/>). All Rights Reserved. THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY RED HAT AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED BY RED HAT. IN NO EVENT SHALL RED HAT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. You may obtain a copy of the source code of the eCos Original Code from <http://www.redhat.com>. You may obtain a copy of source code of Good Technology, Inc.'s Modifications that have been publicly released in Executable form by sending an email to support@good.com. The source code of the eCos Original Code and Good Technology, Inc.'s Modifications are subject to the Red Hat eCos Public License Version 1.1 (copy available at <http://www.redhat.com/>.)

Some or all of the following notices may also apply to portions of the software or documentation provided by Good Technology, Inc.: ScriptEase(tm) Javascript/ECMAScript interpreter developed by Nombas, Inc. All Rights Reserved. This product includes software developed by the Apache Software Foundation (<http://www.apache.org>). Copyright (c) 2000-2003, The Apache Software Foundation and/or Yves Piquet. All rights reserved. Neither the name of Yves Piquet nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0> Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. Copyright (c)1999-

2001 Dan Adler, 315 E72 St. NY, NY, 10021 USA. mailto: danadler@rcn.com All rights reserved. The Jetty Package is Copyright Mort Bay Consulting Pty. Ltd. (Australia) and others. Individual files in this package may contain additional copyright notices. The javax.servlet packages are copyright Sun Microsystems Inc. Copyright (c) 1990-2003 Sleepycat Software. All rights reserved. You may obtain a copy of the source code for the DB software from <http://www.sleepycat.com>. You may obtain a copy of source code of Good Technology, Inc.'s Modifications that have been publicly released in Executable form by sending an email to support@good.com. Copyright ©1996-1999 Corporation for National Research Initiatives; All Rights Reserved. Copyright (c) 1995-2000 by the Hypersonic SQL Group. All rights reserved. Copyright (c) 2001-2002, The HSQL Development Group. All rights reserved. Copyright 2002 (C) Nathaniel G. Auvil. All Rights Reserved. Copyright (c) 1998-2000 World Wide Web Consortium (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. Copyright (c) 2001 MX4J. All rights reserved. Copyright 1994-2005 Sun Microsystems, Inc. All Rights Reserved. Copyright 1999,2000 Boris Fomitchev Copyright 1994 Hewlett-Packard Company Copyright 1996, 97 Silicon Graphics Computer Systems, Inc. Copyright 1997 Moscow Center for SPARC Technology. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>). Copyright (c) 1998-2005 The OpenSSL Project. All rights reserved. THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com). THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software is provided 'as is' with no explicit or implied warranties in respect of any properties, including, but not limited to, correctness and fitness for purpose. Copyright (c) 2002, Cooperative Computers, Inc., Mountain View, CA, USA. All rights reserved. Modifications Copyright (c) J.S.A.Kapp 1994 - 1996. Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind. Copyright (c) 2002,

Cooperative Computers, Inc., Mountain View, CA, USA. All rights reserved. This software is provided 'as is' with no explicit or implied warranties in respect of any properties, including, but not limited to, correctness and fitness for purpose.

Good Technology, Inc. may have patents or pending patent applications, trademarks, copyrights or other intellectual property rights covering this subject matter. The software and documentation do not give you any license to these patents, trademarks, copyrights, or other intellectual property rights except as expressly provided in any written license agreement from Good Technology, Inc. The software and documentation may be covered by one or more patents as set forth at <http://www.rim.net/patents> which have been licensed by Research in Motion, Ltd. ("RIM") to Good. RIM is not affiliated with, nor does RIM endorse the operability of, the products or services described herein. Such patent license should not be construed as exhausting RIM's rights to royalties or damages or other compensation or relief or the grant of any express or implied license: (a) in relation to customer's use of third party products (except to the extent that use of third party email applications arises as a direct result of the customer using Good's products or services or the customer uses a third party wireless personal digital assistant or network carrier services in conjunction with Good's products or services); or (b) where customer or the supplier of the wireless personal digital assistant or wireless network services asserts any intellectual property rights against RIM notwithstanding the terms of clause (a) above, and RIM has exercised its right to suspend all or a portion of the licenses granted to Good.

Disclaimer

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Good Technology, Inc. Information in this document is subject to change without notice. This publication could include technical inaccuracies or typographical errors. Good Technology may make improvements or changes in the products or the programs described in this publication at any time.

Good Technology, Inc.
4250 Burton Drive
Santa Clara, CA, 95054
Tel. (408) 327-6000 Fax (408) 327-6001
www.good.com

Be Good. Be Safe.

Please do not use while driving or engaged in any other activity that requires your full attention.

Contents

- 1 Overview 7**
 - Features and Benefits 7
 - For More Information 8

- 2 Using Good Defense 9**
 - Installing Good Defense 9
 - Upgrading Your Policy 11
 - Managing Your Password 12
 - Unlocking Your Handheld 15
 - What To Do If You Forget Your Password 16
 - Setting Good Defense Options 16
 - Setting Activation, Defense, and Owner Options 16
 - Setting Advanced Options on Palm OS 22
 - Protecting Applications with Passwords 24
 - Encrypting Folders and Volumes 26
 - Encrypting Folders 27
 - Encrypting Volumes 28
 - Encrypting a Database 31
 - Automatic Encryption of New Databases 32
 - Encrypting Storage Cards 33
 - Encrypting a Storage Card on Palm OS Handhelds 35
 - Using Your Phone When Good Defense is Installed 37

Receiving Incoming Calls	38
Making Outgoing Calls	38
Uninstalling Good Defense	39
Uninstalling Good Defense from Palm OS Handhelds	39
Uninstalling Good Defense from Windows Mobile Pocket PC Handhelds	39
Uninstalling Good Defense from Windows Mobile Smartphones.	42
Index	43

1 Overview

Welcome to Good Mobile Defense™. This book is intended for Good Mobile Defense administrators and end users learning how to use the product. This guide describes the features of Good Defense for Windows Mobile and Palm OS handhelds.

Features and Benefits

Good Defense provides complete protection of sensitive data across a variety of handheld platforms. By using Good Defense, Good Messaging, and Good Mobile Intranet, enterprises can increase user uptime, ease system administration, and enforce compliance with corporate security policies and government regulations such as GLB, SB-1386, and HIPAA. A combination of server-side and handheld software, Good Defense provides:

- Advanced Password Management, including protective action after excessive failed password attempts, protection for standard and third-party passwords, and temporary administrative unlock passwords.
- Application Lock-down, including the ability to set and manage approved applications and application launch.
- Handheld Feature Control, including the ability to disable data transfer ports that violate corporate security policies such as Bluetooth, Infrared, or HotSync, and the ability to lock down handheld features such as cameras, microphones, and speakers.

Overview

- Advanced Encryption Management, providing options to control the encryption of native handheld memory, storage cards, and specific applications, using AES 256-bit encryption.
- Data Erase or Lockout after excessive failed password and authentication attempts or when triggered by a security need.

For More Information

For more information about Good Defense and other applications within the Good System product suite, visit www.good.com.

2 Using Good Defense

This chapter provides a basic introduction to using your handheld with Good Mobile Defense (also known as Good Defense). It describes how to install and manage Good Defense. Use the handheld maker's user guide for information on basic operation and care of your handheld.

This chapter includes information about:

- Installing Good Defense
- Upgrading Your Policy
- Managing Your Password
- Unlocking Your Handheld
- Protecting Applications with a Password
- Setting Options
- Protecting the Storage Card
- Using Your Phone When Good Defense is Installed
- Uninstalling Good Defense

Installing Good Defense

The system administrator creates the custom Good Defense policy for you to install on your handheld. The system administrator can specify different policy settings for auto-lock, bitwiping functionality, and database encryption.

Using Good Defense

Good Defense is compatible with handhelds running Palm OS 5.0, (such as Treo 600, 650, and 700p) or Windows Mobile 5.0 handhelds (such as Smartphones and Pocket PC, including the Treo 700w).

If your system administrator has not already installed Mobile Defense on your handheld, the system administrator will send you the Good Mobile Defense installation file over the air if Good Messaging is installed on your handheld or through email.

Installing Good Defense on Palm OS Handhelds

To install the Good Defense setup file (GMDSetup.prc):

1. Over the air: You will receive a Good Messaging notification asking you to install the Good Defense application. Once you have received the Good Defense setup file, select it to install Good Defense.

HotSync: Double-click the Good Defense setup file while your handheld is cabled to your PC and perform a HotSync.

2. Reset your handheld when prompted.

Note: Your handheld may reset several times. Do not interrupt the reset process as this is expected behavior.

3. The first time you use Good Defense, you are prompted to create a password.

Installing on Windows Mobile Handhelds

To install the Good Defense setup file (GMDSetup.ARM.CAB):

1. Over the air: You will receive a Good Messaging notification asking you to install the Good Defense application. Once you have

received the Good Defense setup file, save the file in the My Documents folder and then select it to install Good Defense.

ActiveSync: Connect your handheld to your PC using ActiveSync and move the setup file to the My Documents folder on the handheld. Once the setup file is on your handheld, select it to install Good Defense. If you are prompted to convert the application, select OK.

Note: Do not save the GMDSetup.ARM.CAB file to a storage card when you are prompted to save it.

2. Reset your handheld when prompted.
3. The first time you use Good Defense, you are prompted to create a password.

Upgrading Your Policy

Your IT administrator will update your Good Defense policy as needed. The new policy is included in the GMDPolicyUpgrader.prc file on Palm OS handhelds and in the PDADefSettings.pds file on Windows Mobile handhelds.

Upgrading on Palm OS Handhelds

To upgrade Good Defense:

1. Over the air: You will receive a Good Messaging notification asking you to upgrade the Good Defense application. Once you have received the Good Defense setup file, select it to upgrade Good Defense.

HotSync: Select the GMDPolicyUpgrader.prc file while your handheld is cabled to your PC and perform a HotSync operation.

2. Reset your handheld when prompted.

Upgrading on Windows Mobile Handhelds

To upgrade Good Defense:

1. Over the air: You will receive a Good Messaging notification asking you to install the Good Defense application. If prompted, save the file to the My Documents folder. Once you have received the Good Defense setup file, Good Defense automatically upgrades the application.

ActiveSync: Connect your handheld to your PC using ActiveSync and move the upgrade file to the My Documents folder on your handheld. Once the upgrade file is on your handheld, Good Defense will automatically install it.

2. Reset your handheld when prompted.

Managing Your Password

The system administrator determines your password policies. This policy includes the minimum password length and requirements for letters and digits. The password you select must conform to the password policies included in the policies installed as part of the Good Defense installation file. If a password does not conform to these policies, an error message appears and you are prompted to re-enter the password.

By default the password policy:

- requires a minimum password length of four characters
- requires letters and digits (this includes numbers, spaces, and all special characters)
- expires in 7 days

The password policy sets the amount of time before your password expires. Once your password expires, you are prompted to create a new one.

Note: The password policy set by the IT administrator does not apply to the storage (SD) card password.

If you have forgotten your password, the administrator must reset it for you and assign you a temporary password. For more information, refer to “What To Do If You Forget Your Password” on page 16.

After you install Good Defense, you are prompted to set your password.

Changing Your Password on Palm OS Handhelds

To change your password:

1. Select the **Good Defense** icon on the main Applications screen.
2. When prompted, enter your existing password.
3. Select **Assigned** next to **Password**.
4. Enter your old password.
5. Enter and confirm your new password.
6. Select **OK** to save your password changes.

Changing Your Password on Windows Mobile 5.0 Pocket PC Handhelds

To change your password:

1. From the **Start** menu, select **Settings**, and then the **System** tab.
2. Select **Good Defense**.
3. When prompted, enter your existing password.
4. Select the password box at the top of the page to change your password.
5. Enter your old password.
6. Enter and confirm your new password.
7. Click **OK** to save your password changes.

Changing Your Password on Windows Mobile Smartphones

To change your password:

Using Good Defense

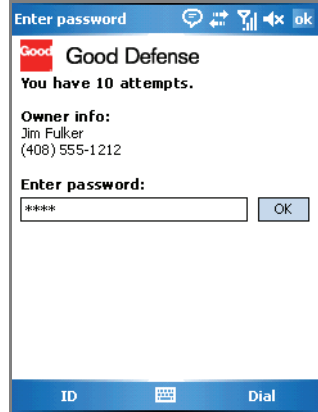
- 1.** From the **Start** menu, select **Good Defense**.
- 2.** Select **Good Defense Settings**.
- 3.** When prompted, enter your existing password.
- 4.** Select **Password Settings**.
- 5.** Select **Change Password**.
- 6.** Enter your old password.
- 7.** Enter and confirm your new password.
- 8.** Click **OK** to save your password changes.

Unlocking Your Handheld

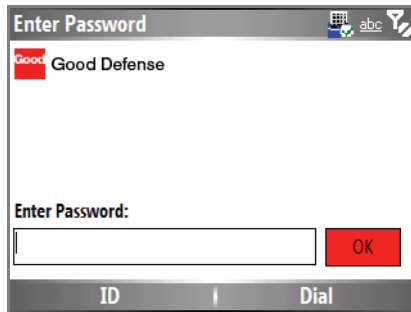
When Good Defense is installed on your handheld, you see the following screen when it is locked:



Good Defense on Palm OS



Good Defense on Windows Mobile



Good Defense on Windows Mobile Smartphone

To unlock your handheld, enter your password and select **OK**.

What To Do If You Forget Your Password

If you have forgotten your password, the IT administrator must reset it for you and assign you a temporary password.

The temporary password is created by your system administrator so you can unlock your handheld within 60 minutes. The specific amount of time given before this temporary password expires is specified by your system administrator. Your system administrator generates the temporary password by using your handheld's ID.

To retrieve the handheld ID:

1. From the main Good Defense lock screen, select **ID**.
2. Give the generated number to your IT administrator so that a new, temporary password can be assigned and used to unlock your handheld.

If your handheld's time is not set to the network time or if you have set it manually, you may also have to give your IT administrator the time and time zone where you are located. The IT administrator has to calculate your handheld's time if your handheld and the system administrator are in different time zones or set to different days.

Setting Good Defense Options

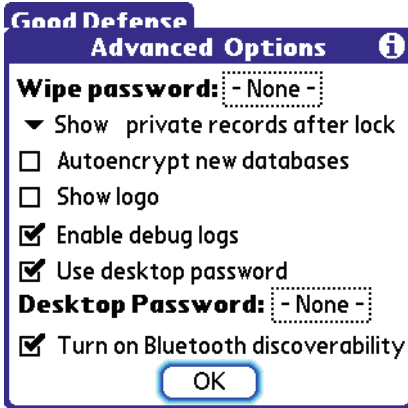
Your handheld includes a number of Good Defense options that you can customize for your use. Your system administrator determines the options you can configure. Some of the options described in this section may not be accessible.

Note: If your IT administrator has not given you permission to access an option, you cannot modify it.

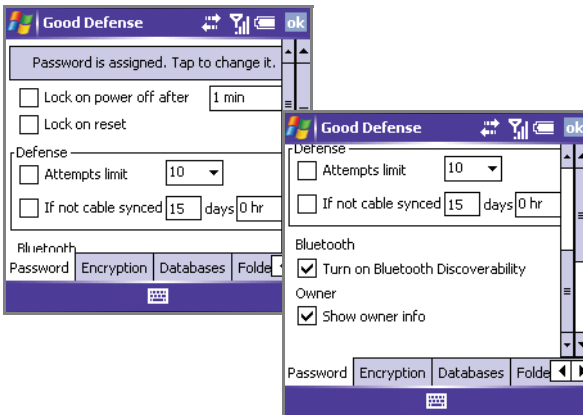
Setting Activation, Defense, and Owner Options

The activation, defense, and owner options let you configure when and how Good Defense is utilized.

To set these options on Palm OS handhelds, select **Options** from the Good Defense main screen. The Good Defense Options screen appears.

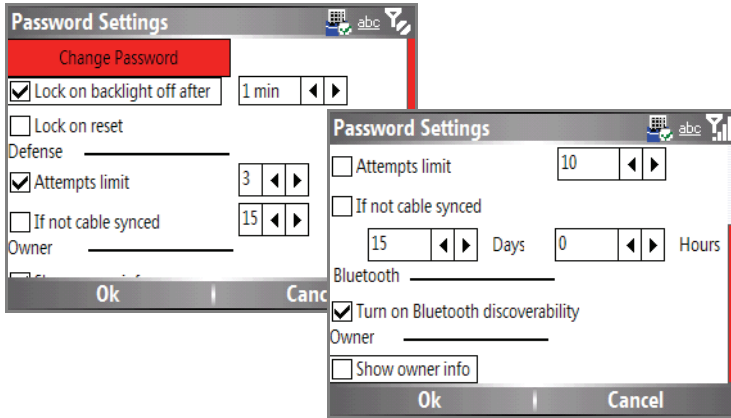


To set these options on Windows Mobile Pocket PC handhelds, select the **Password** tab.



Using Good Defense

To set these options on Windows Mobile Smartphones, select **Password Settings**.



After setting your options, select **OK** to save your changes.

Good Defense Options

Activation Option	Description	Notes
Lock on backlight off after	Automatically activates the lock feature when the backlight shuts off.	Windows Mobile Smartphones only.
Lock on power-off	Automatically activates the lock feature when the handheld's screen is turned off. The handheld is not locked if it is reset. On Windows Mobile Pocket PC handhelds, allows you to set the handheld to delay the activation of the lock feature until the handheld has been turned off (manually or through timeout) for a specified amount of time.	See "If off with time delay" option to set delay on Palm OS handhelds.

Good Defense Options

Lock on reset	Automatically activates the lock feature when the handheld's reset.	Windows Mobile only
Smart	Allows you to have the handheld activate the lock feature when the handheld is turned off, as well as when the handheld is left idle for a specified amount of time. The Lock on power-off option must be enabled to set this option.	Palm OS only
If off with time delay	Allows you to set the handheld to delay the activation of the lock feature until the handheld has been turned off (manually or through timeout) for a specified amount of time. For example, if your handheld turns off after 3 minutes and you have the "If off with time delay" option set to 10 minutes, your handheld will lock after 13 minutes of idle time.	Palm OS only See "Lock on power-off" option to set delay on Windows Mobile handhelds.

Defense Options

Attempts limit	Specifies the maximum number of password attempts allowed before a defense action is triggered by your administrator on your handheld. For example, the database selected for deletion by the administrator can be bitwiped, your handheld may be locked, or the SD card data can be bitwiped.
----------------	--

Using Good Defense

Good Defense Options

If not cable synced Specifies whether Good Defense should engage the wipe or lockout process when a HotSync or ActiveSync operation has not been performed on the handheld after a specified amount of time. If the Good Defense is engaged, the specified defense action is triggered.

Activation of this feature can cause the data on the handheld to be permanently deleted if the bitwipe handheld or bitwipe SD card defenses are set in the policy. If the lockout user defense is set in the policy, the handheld data is preserved. You should periodically perform a HotSync or ActiveSync operation in order to minimize the loss of data in case this feature is activated.

Bluetooth

Good Defense Options

Turn on Bluetooth Discoverability Determines whether or not your handheld can be discovered by another Bluetooth-enabled handheld. If you have established a relationship with another device, it will be able to still communicate with your handheld even if this option is disabled. The partnership ends when the other device is reset. Bluetooth must be enabled first on the handheld or it cannot be turned on by Good Defense. If you disable Bluetooth through Good Defense, it will also disable it in the handheld's settings.

Note: Some handhelds may reset more than once when this option is enabled.

Owner Options

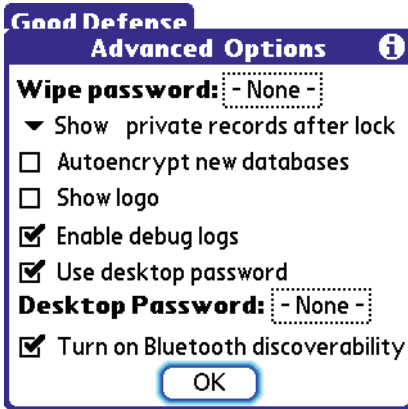
Show owner information Displays all information stored in the owner information within the default OS preference on the Mobile Defense lockout screen.

Stealth mode Stealth mode lets the Good Defense lockout screen mimic the default Palm OS security lockout screen. This feature makes the handheld appear as if it has no advanced security software installed on it. The number of available password attempts is also hidden. Palm OS only

Setting Advanced Options on Palm OS

To set advanced options, select **Advanced** from the Good Defense main screen. The Advanced Options screen appears.

Note: The options below apply to Palm OS handhelds.



Good Defense Advanced Options

Option	Description
Wipe password	Specifies a panic password that, when entered into the lockout screen, engages the bitwipe or erase process. If the administrator has pre-set a panic or defense password, the Wipe Password display is assigned. You can change this password.
Show private records after lock	Specifies whether to show, mask, or hide your private records after the handheld is locked by Good Defense.

Good Defense Advanced Options

Autoencrypt new databases	<p>Selects databases that have been created after the installation of Good Defense. These databases are automatically selected for encryption.</p> <p>Good Defense allows you to manually decrypt all databases that have been selected for encryption by the administrator. Use the Decrypt all databases menu option to do this.</p> <p>This setting is not recommended for Treo handhelds.</p>
Show logo	<p>Displays the custom logo, if set, before the lockout screen. If this option is not selected, the default lockout screen is displayed.</p>
Debug logs enabled	<p>This option is reserved for use as instructed by your customer service representative.</p>
Use Desktop Password	<p>The Desktop Password is the main Palm OS system password used by many other applications and it is used to lock your owner information within the main Palm OS preferences. You are prompted for the desktop password when you synchronize your handheld to your desktop computer.</p> <p>Good Defense does not use the Desktop Password by default.</p>
Turn on Bluetooth discoverability	<p>Determines whether or not your handheld can be discovered by another Bluetooth-enabled handheld. If you have established a relationship with another device, it will be able to still communicate with your handheld even if this option is disabled. The partnership ends when the other device is reset.</p>

After setting your options, select **OK** to save your changes.

Protecting Applications with Passwords

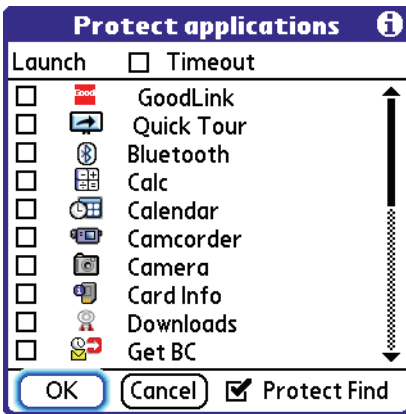
You can configure Good Defense so a password is required before selected applications can be used. If the IT administrator has specified that particular applications be password-protected before they can be started, you cannot change the settings; you can view and add to the list of applications, and on Palm OS handhelds, you can set a timeout value for the protected applications.

Note: If you have Good Messaging installed on the same handheld as Good Defense, disable the Good Messaging password.

Protecting Applications on Palm OS Handhelds

To require a password to start an application:

1. Select Launch from the Good Defense main screen. The Protect Applications screen appears.



2. Select the applications you want to protect with a password. When you start the selected applications, you are prompted for your Good Defense password.

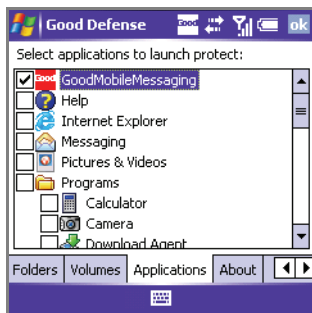
If you select **Protect Find**, the applications are also launch-protected if they appear as a result of a Palm Search. If you locate the applications and they are referenced as shortcuts to the applications, the find results are also launch-protected.

Select **Timeout** to allow a specific amount of time to pass before you re-enter a password-protected application without having to enter your password. For example, if you select Good Messaging and set the time out value to 30 minutes, you are not prompted to enter your password if you go to another application and then return to Good Messaging within 30 minutes.

Protecting Applications on Windows Mobile Pocket PC Handhelds

To require a password to start an application:

1. Select the **Applications** tab from the main Good Defense screen. A list of applications appears.



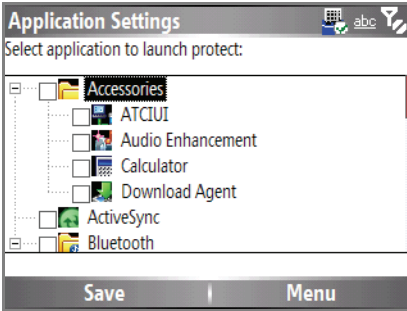
2. Select the applications you want to protect with a password. When you start the selected applications, you are prompted for your Good Defense password.
3. Click **OK** to save your settings.

Note: The Protect Find and Timeout options are not available in the Windows Mobile version of Good Defense.

Protecting Applications on Windows Mobile Smartphones

To require a password to start an application:

1. Select the **Application Settings** from the main Good Defense screen. A list of applications appears.



2. Select the applications you want to protect with a password. When you start the selected applications, you are prompted for your Good Defense password.
3. Click **Save** to save your settings.

Encrypting Folders and Volumes

Note: Folders and volume encryption is only supported on Windows Mobile handhelds.

You can specify folders and volumes to encrypt on Windows Mobile handhelds. When a file, folder, volume becomes encrypted, the information is obscured, unreadable and protected. You can protect individual folders or volumes on your handheld. A volume is part of the file storage available on your handheld and it usually contains a collection of folders and files.

When you encrypt a volume, it provides “always on” encryption and is more secure. Encrypting a volume is quicker and more efficient than encrypting a folder because when a folder is encrypted, every

file in the folder is read and then encrypted or decrypted. When you encrypt a volume, the data in that volume is encrypted at the time it is saved to memory.

If you encrypt a folder, it is encrypted when you lock your handheld and decrypted when you unlock it.

To access a volume, you mount it using your volume password and when it is mounted it is visible for any application to add or delete files from the volume. When the volume is unmounted, the folders in the volume are not protected and not available until you mount the volume again. Other applications cannot save or remove data from the encrypted folders in the volume while it is unmounted.

Note: Encryption settings may be defined by your system administrator and therefore, you may not be able to change these options.

To enable encryption on Windows Mobile Pocket PC handhelds:

1. Select the Encryption tab from the main Good Defense screen.
2. Select Enable encryption. It is enabled by default. If encryption is not enabled, you cannot encrypt databases, folders, or volumes.
3. Click **OK** to save your settings.

Encrypting Folders

When you encrypt a folder, all of the files in that folder are protected when you lock your handheld with Good Defense.

To encrypt a folder on a Window Mobile Pocket PC handheld:

1. Select the **Folder** tab from the main Good Defense screen.
2. Select the folders you want to protect.
3. Click **OK** to save your settings.
4. Optionally, select **Bitwipe Settings** to select the folders you want to bitwipe. The folders you select will be deleted when a bitwipe defense is initiated.

Using Good Defense

Clearing the checkbox means the component will not be encrypted or bitwiped. You can only select a folder that contains data.

To encrypt a folder on Windows Mobile Smartphone:

1. Select the **Folder Encryption** from the main Good Defense screen.
2. Select the folders you want to protect.
3. Click **Save** to save your settings.
4. Select **Folder Bitwipe** from the main Good Defense screen to select the folders you want to bitwipe.

Clearing the checkbox means the component will not be encrypted or bitwiped. You can only select a folder that contains data.

Encrypting Volumes

You can create a secure, encrypted volume. A volume is part of the file storage available on your handheld and it usually contains a collection of folders and files. A volume can also exist on the data storage card. An encrypted volume requires a separate password from your Good Defense password. You can create multiple volumes, up to a maximum of 10.

Volume Options

Option	Description
Volume	Specifies the location
Size	Specifies the storage size, in megabytes, of the part of the storage card you want to encrypt. The amount must be equal or less than the free space on the card or in main memory.
Encryption	Specifies the type of encryption used to protect the storage card. By default, Good Defense includes the encryption provider AES. AES key length is 256-bit.
Password/Confirm	Specifies and confirms your volume password.

Volume Options

Name	Specifies the name of the encrypted volume.
Folder	Specifies the folders to be included in the encrypted volume.
Type	Specifies the type of volume. By default, the type is Good Mobile Defense disk (.dsk).
Location	Specifies the location of the encrypted volume.

Creating a Volume on Windows Mobile Pocket PC Handhelds

To create a volume:

1. Select the **Volumes** tab from the main Good Defense screen.
2. Select **File** and then **New**.
3. Select the ellipsis (...) next to the **Volume** field.

You do not need to enter any text in the Volume field on this screen. It will be populated automatically with the folder location after you provide more information on the next screen.
4. Enter a name for the volume.
5. Specify which folders you want to include in the volume.
6. Specify the type of volume. In this case, you can only choose Good Defense disk. The volume created has the file type extension .dsk.
7. Choose the location. The location can be in main memory, storage card or within another volume.
8. Select **Save**.
9. Specify the size of the volume.

The size you specify for the volume is subtracted from the total free space available on the handheld.
10. Enter and confirm a password. This password is used to access (mount and decrypt) the volume.
11. Click **OK** to save your settings.

Using Good Defense

Creating a Volume on Windows Mobile Smartphones

To create a volume:

1. Select **Volumes** from the main Good Defense screen.
2. Select **File** and then **New**.
3. Specify the volume's path.
4. Enter a name for the volume.
5. Specify the size of the volume.
The size you specify for the volume is subtracted from the total free space available on the handheld.
6. Enter and confirm a password. This password is used to access (mount and decrypt) the volume.
7. Click **OK** to save your settings.

Deleting a Volume on a Windows Mobile Pocket PC Handheld

To delete a volume:

1. Select the **Volumes** tab from the main Good Defense screen.
2. Select **Delete** from the **File** menu. If the file is mounted, you must dismount before the volume can be deleted. Select **Dismount** from the **Volume** menu to do this.

Deleting a Volume on a Windows Mobile Smartphone

To delete a volume:

1. Select **Volumes** from the main Good Defense screen.
2. Select **Delete** from the **File** menu. If the file is mounted, you must dismount before the volume can be deleted. Select **Dismount** from the **Volume** menu to do this.

Adding a File or Volume Through Beaming

You can add a file or volume that another user has beamed to you to those volumes that are protected by Good Defense.

To add a file or volume:

1. Select the **Volumes** tab from the main Good Defense screen.
2. Select **Add** from the file menu and navigate to the directory where the existing Good Defense disk (.dsk) file is located.
3. Select the folders, by tapping the names, you want to add to the secure volume. By default, Good Defense searches for secure volume files.
4. Click **OK**.

Mounting and Dismounting a Volume on Windows Mobile Pocket PC Handhelds

To mount or dismount a volume:

1. Select the **Volumes** tab from the main Good Defense screen.
2. Select **Mount** or **Dismount** from the **Volume** menu.

When a volume is mounted, the information in it is available to other applications and is not protected. When it is dismounted, the information in it is encrypted and not available.

Mounting and Dismounting a Volume on Windows Mobile Smartphones

To mount or dismount a volume on Smartphones:

1. Select the **Volumes** from the main Good Defense screen.
2. Select **Mount** or **Dismount** from the **Volume** menu.

When a volume is mounted, the information in it is available to other applications and is not protected. When it is dismounted, the information in it is encrypted and not available.

Encrypting a Database

You can encrypt a database or bitwipe it.

Using Good Defense

Encryption a Database on Windows Mobile Pocket PC Handhelds

To select a database for encryption or bitwiping:

1. Select the **Database** tab from the main Good Defense screen.
2. Select the database you want to protect.
3. Select **Bitwipe Settings** to select the databases you want to bitwipe.

Clearing the checkbox means the component will not be encrypted or bitwiped. You can only select a database that contains records.

Encryption a Database on Windows Mobile Smartphones

To select a database for encryption on Smartphone:

1. Select the **Database Encryption** from the main Good Defense screen.
2. Select the database you want to protect.
3. Select **Save**.

To select a database for bitwiping on Smartphone:

1. Select **Database Bitwipe** from the main Good Defense screen.
2. Select the database you want to bitwipe.
3. Select **Save**.

Clearing the checkbox means the component will not be encrypted or bitwiped. You can only select a database that contains records.

Automatic Encryption of New Databases

You can have Good Defense automatically encrypt any new databases and applications that are added to the handheld during the syncing process. To activate this option, select the checkbox next to "Auto encrypt new databases."

Note: If you choose to enable auto encryption, it can cause third party software conflict errors. Some applications do not operate correctly when Good Defense encrypts their databases. If they are installed onto a handheld with Good Defense and auto encryption is enabled, then a third-party application conflict may arise.

Encrypting Storage Cards

You can also use Good Defense to protect the information stored on the handheld's data storage (SD) card. Good Defense protects the storage card by encrypting the information on it. If you have a Good Messaging backup on your storage card, leave 3 to 4 MB free. Your IT administrator may set a policy to force data storage card encryption.

Note: A message referring to an "external device" may appear while encrypting the storage card. The "external device" is the storage card.

If a storage card is inserted into the handheld, and the force storage card encryption policy is set, you are prompted to allow Good Defense to format the card. If you select Cancel, the card cannot be used. This means that the card is unmounted and you cannot access (read or write to) it.

Important: You are prompted to delete the contents of your storage card when you choose to encrypt your storage card.

Encrypting a Storage Card on Windows Mobile Pocket PC Handhelds

When you want to protect the storage card for a Windows Mobile handheld, you create a volume on the storage card and encrypt that volume.

To encrypt a storage card on Windows Mobile Pocket PC handhelds:

Using Good Defense

1. Select the **Volumes** tab from the main Good Defense screen.
2. Select **File** and then **New**.
3. Select the ellipsis (...) next to the **Volume** field.
You do not need to enter any text in the Volume field on this screen. It will be populated automatically after you provide more information on the next screen.
4. Enter a name for the volume.
5. Specify which folders you want to include in the volume.
6. Specify the type.
7. Choose the location of the storage memory card from the drop-down menu.
8. Select **Save**.
9. Specify the size of the encrypted volume you want to create.
10. Assign a volume and confirm it.
11. Select **OK**. The new volume is created.
12. The password screen appears. To mount the newly created volume, enter the password. Otherwise, select **Cancel**.

Encrypting a Storage Card on Windows Mobile Smartphones

1. Select **Volumes** from the main Good Defense screen.
2. Select **File** and then **New**.
3. Specify the path of the storage card.
4. Enter a name for the volume.
5. Specify the size of the volume.
The size you specify for the volume is subtracted from the total free space available on the handheld.
6. Enter and confirm a password. This password is used to access (mount and decrypt) the volume.
7. Click **OK** to save your settings.

For more information about creating an encrypted volume, see “Encrypting Volumes” on page 28.

Encrypting a Storage Card on Palm OS Handhelds

On Palm OS handhelds, you can access or mount both protected and unprotected portion of the storage card. You can access the protected portion of the card by providing the card password.

If your system administrator sets a policy that forces storage card encryption, you are required to reformat the entire storage card upon initial insertion, completely removing all data from the card.

Otherwise, the card is not usable, regardless of the Card Manager settings in Good Defense on the handheld. If this option is set, you cannot use the Format Card option.

Unprotecting a card using Card Manager removes all protected data from the card. Information added to any unprotected portion of the card is not affected by unprotecting the card.

When you insert a protected card, you are prompted for your Good Defense password. If you choose Cancel, protected volumes on the card are not available. To mount all volumes, including those on the storage card, select Mount All Volumes from the Options menu.

To encrypt the storage card on Palm OS handhelds:

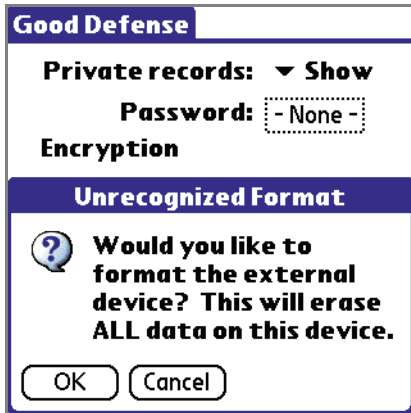
Using Good Defense

1. Select Card Manager from the Good Defense main screen. The Card Manager screen appears.



2. Select the name of the data storage card to encrypt.
3. Specifies the type of encryption used to protect the storage card. By default, Good Defense includes the encryption provider AES. AES key length is 256-bit.
4. Specifies the storage size, in kilobytes, of the part of the storage card you want to encrypt. The amount must be equal or less than the free space on the card.
5. Select **Protect** to encrypt the storage card.
6. Enter a new card password and confirm it.

7. An alert appears asking you to format the external device. Click **OK** to continue.



This alert appears when a card that has not been protected is detected. The formatting applies to the portion of the storage card you want to encrypt. The rest of the storage card is not formatted.

8. The next time you insert the card, you are prompted for the password. If you select **Cancel** instead of entering the password, you cannot view the contents of the card.
9. To decrypt the information on the storage card, select **Unprotect** from the Card Manager screen.

Using Your Phone When Good Defense is Installed

When you have Good Defense installed and your handheld is locked, you can still use the phone to make calls. Select **Dial** from the System Lockout screen to use the phone. If you have selected the phone as a launch-protected application, you are prompted for your password before you proceed. If you receive a call while your handheld is locked, you do not have to enter your password to answer the call.

Receiving Incoming Calls

When you receive a call when your handheld is locked, an incoming call notification is displayed with the caller's ID and the options to either ignore or answer the call. The call progress screen is moved to the background if you answer the call.

You can access your Phone Favorites list and Call History. You do not have access to Contacts or other applications. Selecting other applications returns you to the Lock screen.

8125 and Apache

The call progress screen can be displayed by using one of the following:

- Phone hardware button
- Dial button on the screen
- Unlocking the lock screen

Treo 700

The call progress screen can be displayed only by unlocking the lock screen. Pressing the phone hardware button or selecting Dial takes you to the Dialer screen again.

Making Outgoing Calls

Select the Dial soft button or phone hardware button to display the Dialer screen.

Motorola Q, 8125, and Apache:

The call progress screen is displayed during the call.

Treo 700

Pressing the Control key returns to the lock screen during the call. Unlocking the lock screen returns to the call progress screen.

Uninstalling Good Defense

You must have administrator privileges to uninstall Good Defense from the handheld.

Uninstalling Good Defense from Palm OS Handhelds

To uninstall Good Defense:

1. Select the Good Defense icon on the Applications screen to start the application.
2. Enter the administrator password when prompted for your password. When you have successfully logged in as the administrator, a dialog appears on the handheld:



3. Palm OS: Select **Uninstall** from the Options menu.
4. Confirm you want to uninstall Good Defense.

Uninstalling Good Defense from Windows Mobile Pocket PC Handhelds

When you uninstall Good Defense from Windows Mobile handhelds, you must first clear all of the passwords before you can remove the program.

To uninstall Good Defense:

1. From the **Start** menu select **Programs** and then **Good Defense** folder.
2. Select the Good Defense icon.

Using Good Defense

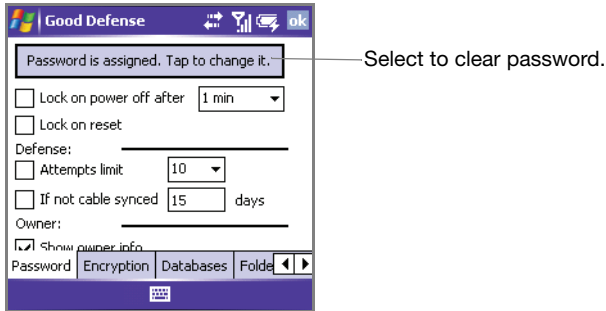
3. Enter the Administrator password. A dialog confirming that you are logged in as the administrator appears.



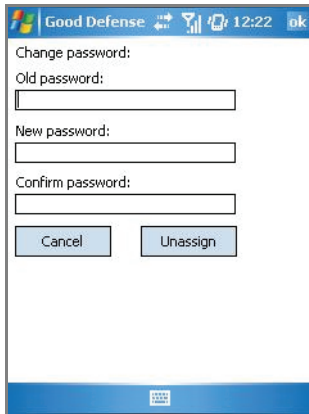
4. Click **OK**. The main Good Defense screen appears.



- From the **Password** tab, select **Password is assigned** to change password.



- Select **Unassign** and then **Yes** to confirm that you want to clear all passwords.



- Click **OK**.
- If any volumes are mounted, dismount them.
- From the Start menu, select **Settings** and then the **System** tab.
- Select **Remove Programs**.
- Select **Good Technology Good Defense**.

Using Good Defense

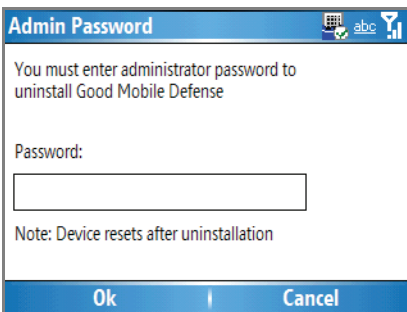
12. Enter the administrator password.
13. Confirm that you want to remove Good Defense.

Uninstalling Good Defense from Windows Mobile Smartphones.

1. Select **Settings** folder from **Start** menu.
2. Select **Remove Programs**.
3. Select **Good Technology Good Defense**.



4. Confirm that you want to remove Good Defense.



5. Enter the administrator password to remove Good Defense. The handheld resets after Good Defense is removed.

Index

Numerics

256-bit encryption 8

A

activation options 16
advanced options 22
AES 8
After 18
applications, password
 protecting 24
attempts limit option 19
autoencrypt databases option 23

B

benefits 7

C

cabled sync option 20
calls, making 38
card manager options 36
changing passwords 13

D

data storage card 33
defense options 16, 19

E

encrypting
 folders 26, 27
 storage cards 33
 volumes 26

F

features 7
folders
 encrypting 27

G

GMDSetup.ARM.CAB 10
GMDSetup.prc 10
Good Defense icon 39
Good Defense, installing 9

H

handheld ID 16
handheld, unlocking 15

I

ID of handheld 16
If off with time delay 19
installation 9

L

lock on power-off 18
lock on reset option 19
logo, show 23

M

making calls 38

O

on Palm OS handhelds 11
options 16, 22
 advanced 22
 attempts limit 19

Index

- autoencrypt new databases 23
- cabled sync 20
- card manager 36
- defense 19
- if off with time delay 19
- lock on power-off 18
- lock on reset 19
- owner 21
- setting 16
- show logo 23
- show private record 22
- smart lock 19
- stealth mode 21
- time delay 18
- volume 28
- who owner information 21
- owner options 16, 21

P

- passwords 12
 - changing on Palm OS handhelds 13
 - changing on Windows Mobile handhelds 13
 - for application launch 24
 - temporary 16
 - wipe 22
- phone, using with Good Defense 37
- protecting applications
 - on Palm OS handhelds 24
- protecting applications on Windows Mobile handhelds 25
- protecting data storage cards 33

S

- SD card 33
- setting options 16
- show logo option 23
- show owner information option 21
- show private record option 22
- smart lock 19
- stealth mode option 21

T

- temporary password 16
- time delay option 18

U

- uninstalling Good Defense 39
- unlocking the handheld 15
- upgrading 11
- using phone with Good Defense installed 37

V

- volume options 28

W

- where to go for more information 8
- wipe password 22