Security 5.0p Guide for the Palm™ Tungsten™ T3 Handheld

Copyright

© 2002-2003 Palm, Inc. All rights reserved. Graffiti, HotSync, the Palm logo, Palm OS, and the Palm Powered logo are registered trademarks of Palm, Inc. Palm, Tungsten, VersaMail, and Zire are trademarks of Palm, Inc. Palm, Inc. uses the Bluetooth trademark under express license from the owner. All other brands are trademarks or registered trademarks of their respective owners.

Disclaimer and Limitation of Liability

Palm, Inc. assumes no responsibility for any damage or loss resulting from the use of this guide.

Palm, Inc. assumes no responsibility for any loss or claims by third parties which may arise through the use of this software. Palm, Inc. assumes no responsibility for any damage or loss caused by deletion of data as a result of malfunction, dead battery, or repairs. Be sure to make backup copies of all important data on other media to protect against data loss.

IMPORTANT Please read the End User Software License Agreement with this product before using the accompanying software program(s). Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

PN: 407-6256A-ML

POWERED

Contents

About This Book **1**

About Security 5.0p **3**

Assigning a password 3

Changing or deleting a password 4

Assigning a Quick Unlock combination 5

Changing or deleting your Quick Unlock combination 6

Locking your handheld 7

Locking your handheld automatically 7

Locking your handheld manually 8

Recovering from a forgotten password 9

Making records private 10

Encrypting your data 11

Encrypting only private records in the selected applications 12

Setting the encryption algorithm 12

Setting intrusion protection 13

About This Book

The *Security 5.0p Guide for the Palm™ Tungsten ™ T3 Handheld* is based on the following assumptions:

- You are using a Palm Tungsten T3.
- You have installed Security 5.0p.
- You know how to use the basic functions of your handheld, such as the basic applications and HotSync® technology.
- You know how to enter text and select onscreen items using the available controls on your handheld, such as a built-in keyboard, an input area, an icon area, or a navigator button.
- You are familiar with existing features of the Security preferences that comes on your Palm Tungsten T3.

For information about any aspect of your handheld, please consult the *Handbook for Palm™ Tungsten™ T3 Handheld* and other documentation that came with your Palm Tungsten T3, or go to www.palm.com/support. If you are outside the United States, go to www.palm.com/support/intl.

About Security 5.0p

Palm™ Tungsten™ T3 Security preferences keep the data on your handheld safe. Security 5.0p is an upgrade to the current Security preferences and adds powerful new features:

- Quick Password Entry

  Unlock your handheld by entering a Quick Unlock combination with one hand using the navigator buttons.

- Data encryption

  Ensure the confidentiality of your handheld data with encryption. Once the handheld is locked, your data remains encrypted until the correct password is entered. You can encrypt all of your data or only selected applications. Your choice of algorithms includes AES (Advanced Encryption Standard) or RSA Security's RC4.

- Intrusion protection

  Limit the number of failed password attempts to prevent a dictionary attack by an intruder.

- FIPS-certified cryptography

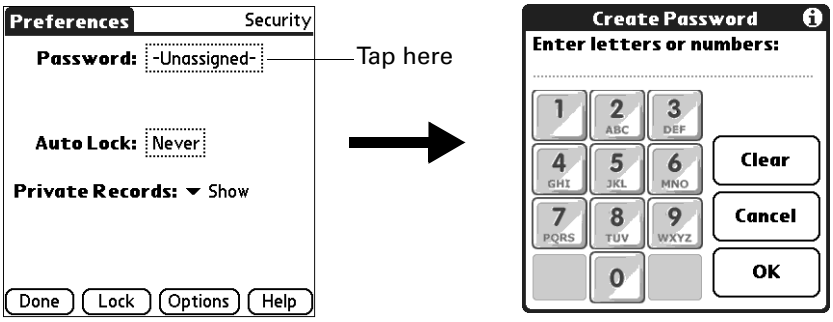
  Our AES implementation is FIPS 140-2 certified.

Assigning a password

You can assign a password to protect your private records and to lock your handheld. Any combination of letters, characters, and numbers can be used to create your password.

To assign a password:

1. From the General Preferences list, select Security.
2. Tap the Password box.



3. Enter a password using one or more of the following:
   - Numeric keypad located in the Create Password dialog box
   - Graffiti® 2 writing and the onscreen keyboard located in the input area
   - Full-screen Writing
4. Tap OK.
5. Enter the same password to confirm and tap OK.
6. (Optional) Enter a hint to help you remember your password if you forget it.
7. Tap Done.

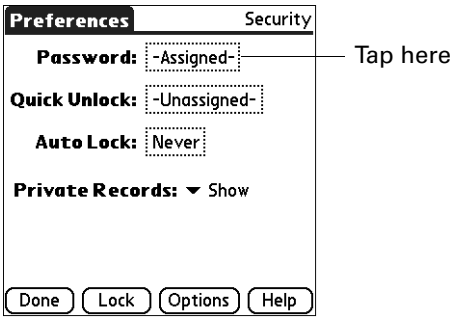
The Password status indicates Assigned.

Changing or deleting a password

Once you define a password for your handheld, you can change or delete it at any time.

To change your password:

1. From the General Preferences list, select Security.
2. Tap the Password box.



3. Enter your password and tap OK.

   NOTE If you already entered your password in your current session using Security preferences, the password dialog box does not appear. You need to enter your password only once during a session in the Security preferences to change security settings.

4. Tap OK.

5. Enter a password using one or more of the following:
   - Numeric keypad located in the Create Password dialog box
   - Grafitti 2 and the onscreen keyboard located in the input area
   - Full-screen Writing
6. Tap OK.
7. Enter the same password to confirm and tap OK.
8. (Optional) Enter a hint to help you remember your password if you forget it.
9. Tap Done.

The Password status indicates Assigned.

To delete your password:

1. From the General Preferences list, select Security.
2. Tap the Password box.
3. Enter your password and tap OK.

   NOTE If you already entered your password in your current session using Security preferences, the password dialog box does not appear. You need to enter your password only once during a session in the Security preferences to change security settings.

4. Tap Unassign.

The Password status indicates Unassigned.

Assigning a Quick Unlock combination

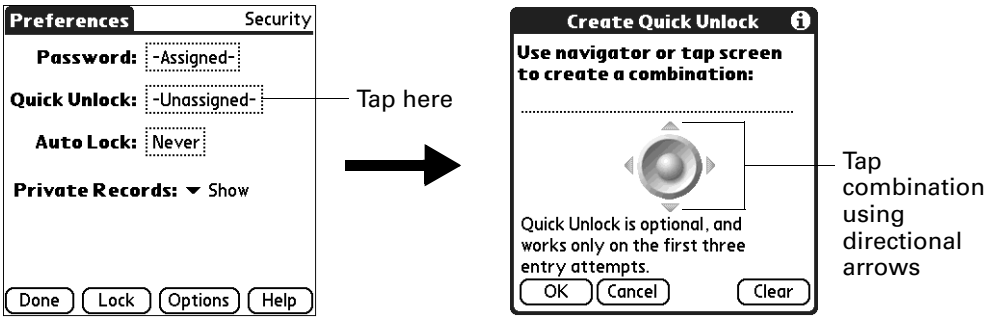
To quickly log in, you can also assign a Quick Unlock combination that uses the navigator buttons. Quick Unlock works only with your first three login attempts.

IMPORTANT When using your Quick Unlock combination to unlock your handheld, you must tap OK or press the center navigation button to submit your combination.

To assign a Quick Unlock combination:

1. From the General Preferences list, select Security.
2. Tap the Quick Unlock box.

The Quick Unlock option appears only if you have assigned a password.



3. Use the navigator directional buttons or tap the screen to create a combination.
4. Perform one of the following to submit your combination:
   - Tap OK.
   - Press the center navigator button.
   - Tap the onscreen center navigator button.

The Quick Unlock status indicates Assigned.

Changing or deleting your Quick Unlock combination

You can change or delete your Quick Unlock combination at any time.

To change or delete your Quick Unlock combination:

1. From the General Preferences list, select Security.
2. Tap the Quick Unlock box.
3. Enter your password and tap OK.

   NOTE If you already entered your password in your current session using Security preferences, the password dialog box does not appear. You need to enter your password only once during a session in the Security preferences to change security settings.

4. Perform one of the following:
   - Use the navigator buttons or tap the screen to create a new Quick Unlock combination. Tap or press the center navigator button or tap OK.
   - Tap OK without entering a combination to delete the Quick Unlock combination.

Locking your handheld

You can lock your handheld so that it cannot be operated until your password or Quick Unlock combination is entered. In the event that your handheld is lost or stolen, this helps protect your data from unauthorized use. You can set your handheld to lock automatically, or you can lock it manually.

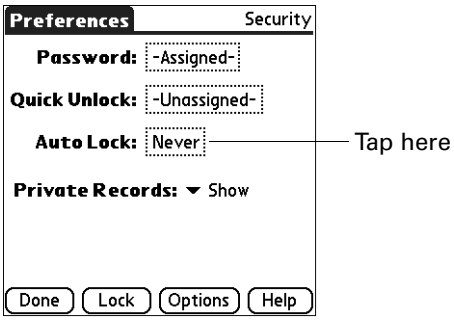
Locking your handheld automatically

You can set your handheld to lock automatically when any one of the following occurs:

- When you turn off the power
- At a time you specify
- After a period of inactivity you specify

To set your handheld to lock automatically:

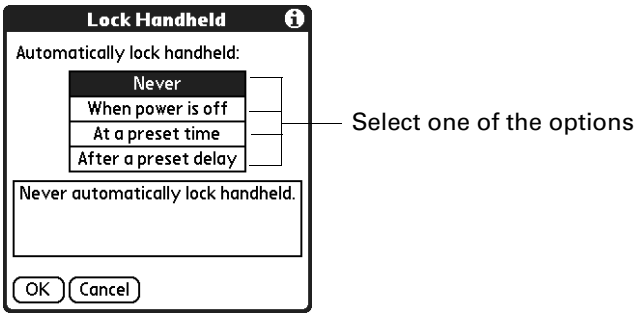
1. From the General Preferences list, select Security.
2. Tap the Auto Lock box.



3. Enter your password and tap OK.

NOTE If you already entered your password in your current session using Security preferences, the password dialog box does not appear. You need to enter your password only once during a session while in the Security preferences to change security settings.

4. Select one of the options.



Never	Handheld is never automatically locked.
When power is off	Automatically locks handheld when power is turned off.
At a preset time	Locks the handheld at the time set in the Set Time dialog box. The Set Time dialog box automatically opens so that you can use the arrows to set the time.
After a preset delay	Automatically locks handheld when inactive for the set length of time. Enter the inactive period, and then select Minute(s) or Hour(s) from the pick list.

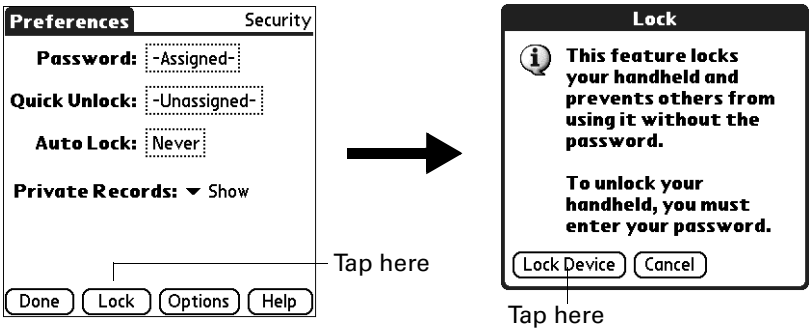
5. Tap OK.

Locking your handheld manually

You can turn off and lock your handheld manually.

To lock and turn off your handheld:

1. From the General Preferences list, select Security.
2. Tap Lock.



3. Tap Lock Device.

Recovering from a forgotten password

Recovering from a lost password is different depending on whether or not you are locked out of your handheld.

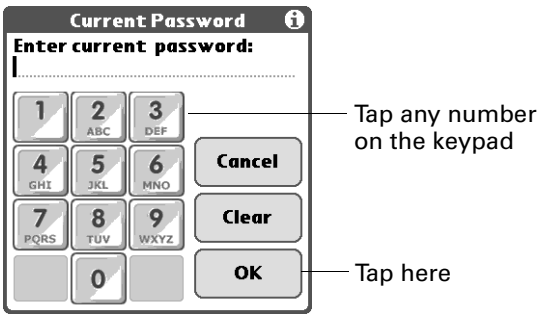
If you are not locked out of your handheld

If you are *not* locked out of your handheld and you forget your password, your handheld displays a hint, if you entered one, to help you remember the password. If you are still unable to remember the password, you can delete it from your handheld.

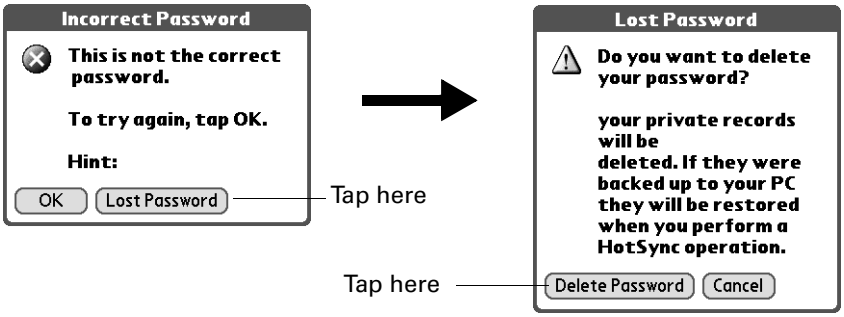
IMPORTANT Deleting a forgotten password also deletes all Private records from your handheld. If you synchronize with your computer before deleting a forgotten password, your handheld restores your private entries the next time you perform a HotSync operation, but it does not restore the password.

To delete your password:

1. From the General Preferences list, select Security.
2. Tap Password box.
3. Tap any number on the keypad and tap OK.



4. Tap Lost Password.



5. Tap Delete Password.

Your password and all private records are deleted from your handheld. The Password status indicates Unassigned.

If you are locked out of your handheld

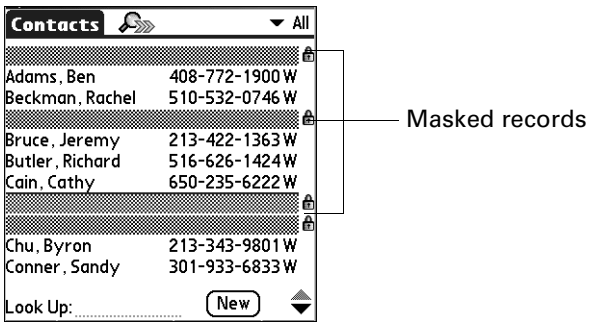
If you locked your handheld, you must enter the exact password to reactivate your handheld. If you forget the password, your handheld presents the hint you have entered to help you remember the password.

If you still cannot remember the password, you must perform a hard reset to resume using your handheld. Performing a hard reset deletes all the records in your handheld; however, you can restore all synchronized data at the next HotSync operation. See Appendix A of your *Handbook for Palm™ Tungsten™ T3 Handheld* for more information on performing a hard reset.

Making records private

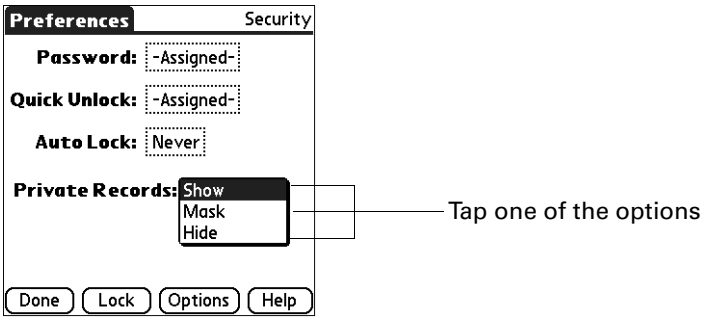
In many applications, you can make individual records private. Private records remain visible and accessible until you select the Security setting to hide or mask all private records.

Masked records appear as gray placeholders in the same position they would appear if they were not masked, and are marked with a lock icon. Hidden records disappear completely from the screen. If you define a password for your handheld, you must enter it to display private records.



To show, hide, or mask all private records:

1. From the General Preferences list, select Security.
2. Tap the Private Records pick list and select from the pick list.



Show	Private records are visible and accessible.
Mask	Private records appear as gray placeholders in the same position they would appear if they were not masked, and are marked with a lock icon.
Hide	Hidden records disappear completely from the screen.

3. Tap Done.

Encrypting your data

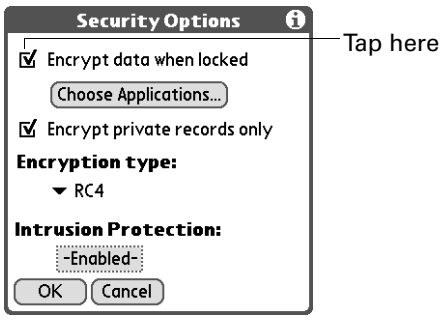
You can encrypt selected data whenever your handheld locks. You can choose to encrypt the data in selected applications. The more applications and data that are selected, the longer the encryption process.

When you unlock the handheld and enter a valid password, the encrypted data is decrypted. The more applications and data that are selected for encryption, the longer the decryption process.

If you select an application that uses very large files, such as Palm Photos, the message appears: *Encrypting this application may affect performance*. You can proceed with encryption, but be aware that very large files create long encryption and decryption times. When encrypting these files, consider the security versus convenience trade-off.

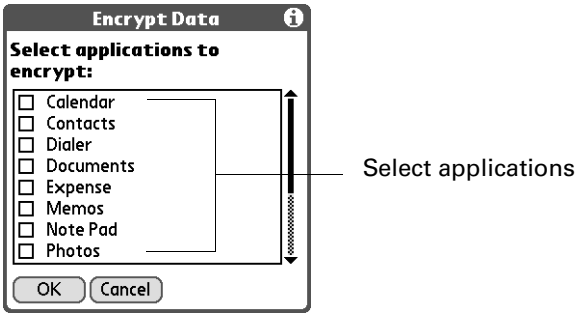
To encrypt data in selected applications when the handheld locks:

1. From the General Preferences list, select Security.
2. Tap Options.
3. Select the Encrypt data when locked check box.



4. Tap the Choose Applications button.
5. Select the applications whose data you want to encrypt, and tap OK.

You must select at least one application.



6. Tap OK on the Security Options dialog box.

Encrypting only private records in the selected applications

To help shorten the encryption and decryption process, you can choose to encrypt only the private records in the applications you selected when you tapped the Choose Applications button.

To encrypt only private records in the selected applications when the handheld locks:

1. From the General Preferences list, select Security.
2. Tap Options.
3. Select Encrypt private records only and tap OK.
4. Tap OK on the Security Options dialog box.

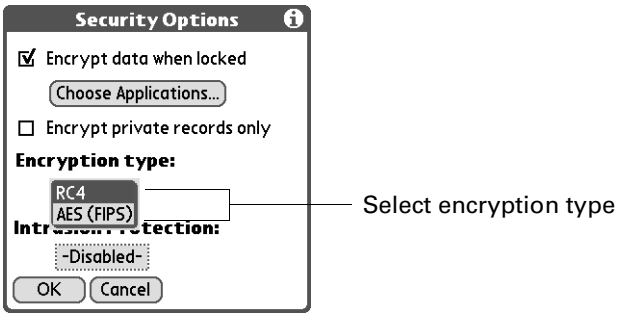
Setting the encryption algorithm

You can also choose the encryption algorithm used to encrypt your data

To set the type of data encryption used:

1. From the General Preferences list, select Security.
2. Tap Options.

3. Tap the Encryption type pick list and select an encryption type.



RC4	RC4 is a symmetric algorithm created by RSA Security, Inc. Our implementation of RC4 uses a 128-bit symmetric key.
AES (FIPS)	AES (Advanced Encryption Standard or Rijndael) is a FIPS-approved symmetric encryption algorithm. Palm's implementation of AES uses a FIPS 140-2 certified cryptographic library and a 128-bit key.

NOTE For faster performance during encryption and decryption, choose RC4 rather than AES (FIPS). If your workplace requires FIPS-certified encryption, then choose AES (FIPS).

4. Tap OK and then tap OK on the Security Options dialog box.

Setting intrusion protection

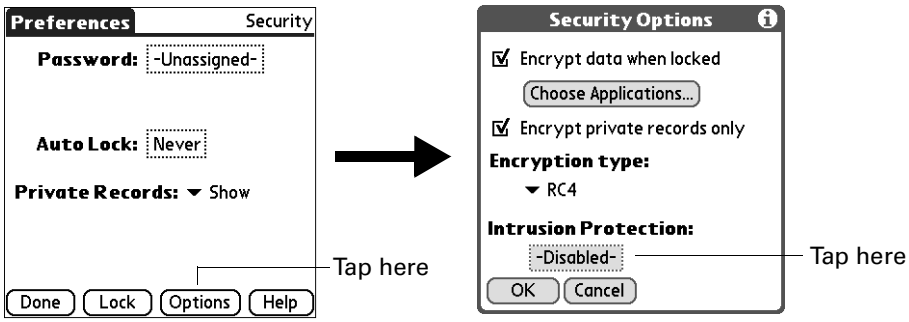
You can set the number of incorrect password attempts before all data is deleted from the handheld. This feature protects sensitive data from an intruder using a *dictionary attack*, also known as a brute force attack, to gain access to the device. This attack method refers to when the intruder uses an automated means to attempt every possible combination until the password is found. Data is *zeroed-out*, meaning an intruder cannot recover the deleted data using forensic techniques.

TIP Back up data frequently to prevent loss of data in the event intrusion protection is triggered.

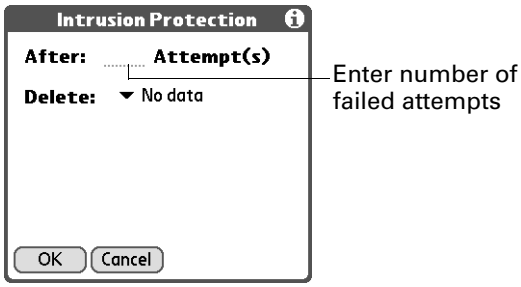
IMPORTANT To prevent accidental password entry attempts while the handheld is in a purse or pocket, use the Keylock preference. See the Preferences chapter of your *Handbook for Palm™ Tungsten™ T3 Handheld* for more information.

To set your intrusion protection parameters:

1. From the General Preferences list, select Security.
2. Tap Options.



3. Tap the Intrusion Protection box.



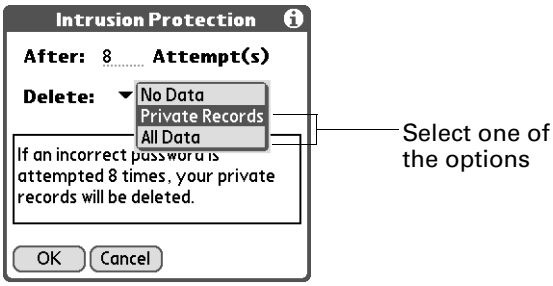
4. Enter the number of failed attempts before intrusion protection is triggered.

   Valid options are a minimum of 5 and a maximum of 99.

   NOTE Failed Quick Unlock password attempts are not counted as failed attempts by the intrusion protection counter.

5. Tap the Delete pick list to select the action that occurs when intrusion protection triggers.

   If you do not choose an action, intrusion protection is disabled.



No Data	No data is deleted. This is the default selection. **NOTE** If No Data is selected, intrusion protection is disabled.
Private Records	Deletes all private records on the handheld. **NOTE** A message informs you of the data deletion after your first successful login following the deletion of private records.
All Data	Deletes all user data and user-installed applications on the handheld, returning the handheld to the factory default condition. **NOTE** No message informs you of the data deletion after your first successful login following the deletion of all data. The deletion is obvious because your handheld is in the factory default condition.

6. Tap OK.
7. Tap OK on the Confirmation screen.

The Intrusion Protection status indicates Enabled.