Software License Agreement

The following is a copy of the Software License Agreement as shown in the software:

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE LOADING THE SOFTWARE. THIS AGREEMENT GOVERNS THE USE OF THE SOFTWARE (AS DEFINED BELOW). BY CLICKING "I ACCEPT" BELOW, OR BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE, YOU ARE SIGNING THIS AGREEMENT, THEREBY BECOMING BOUND BY ITS TERMS. BY INDICATING YOUR AGREEMENT, YOU ALSO REPRESENT AND WARRANT THAT YOU ARE A DULY AUTHORIZED REPRESENTATIVE OF THE ENTITY THAT HAS PURCHASED THE SOFTWARE AND THAT YOU HAVE THE RIGHT AND AUTHORITY TO ENTER INTO THIS AGREEMENT ON THE ENTITY'S BEHALF. IF YOU DO NOT AGREE WITH THIS AGREEMENT, THEN CLICK "I DO NOT ACCEPT" BELOW OR DO NOT USE THE SOFTWARE AND RETURN ALL COPIES OF THE SOFTWARE AND DOCUMENTATION TO ALADDIN OR THE RESELLER FROM WHOM YOU OBTAINED THE SOFTWARE.

1. DEFINITIONS.

1.1 "Documentation" means the published user manuals, User Guide and any additional documentation that are made available for the Software.

1.2 "Software" means the machine-readable object-code version of Aladdin's SafeWord software including any revisions, corrections, modifications, enhancements, updates and/or upgrades thereto that you may receive.

2. GRANT OF LICENSE. Aladdin grants to you, and you accept, a personal, nonexclusive, non-transferable and fully revocable limited license to use the Software, in executable form only, for a predefined set number of licensed users, as described in the Software accompanying Documentation and only according to the terms of this Agreement. Under no circumstances will you receive any source code of the Software. Aladdin also grants to you, and you accept, a non-exclusive, and non-transferable limited license to use the Documentation solely in conjunction with the Software.

3. LIMITATION OF USE. You may not: 1) copy the Software, except to make one copy of the Software solely for back-up or archival purposes; 2) transfer, distribute, rent, lease or sublicense all or any portion of the Software or Documentation to any third party; 3) translate, modify, adapt, decompile, disassemble, or reverse engineer any Software in whole or in part; 4) modify or prepare derivative works of the Software or the Documentation; or 5) use the Software to process the data of a third party; 6) place the Software onto a server so that it is accessible via a public network; and 7) use any back-up or archival copies of the Software (or allow someone else to use such copies) for any purpose other than to replace an original copy if it is destroyed or becomes defective. You agree to keep confidential and use your best efforts to prevent and protect the contents of the Software and Documentation from unauthorized disclosure or use. Aladdin reserves all rights that are not expressly granted to you. If you are a member of the European Union, this agreement does not affect your rights under any legislation implementing the EC Council Directive on the Legal Protection of Computer Programs. If you seek any information within the meaning of that Directive you should initially approach Aladdin.

4. DISCLAIMER OF WARRANTIES. Aladdin does not warrant that the functions contained in the Software will meet your requirements or that operation of the program will be uninterrupted or error-free. The entire risk as to the results and performance of the Software is assumed by you. THE SOFTWARE IS FURNISHED, "AS IS" WITHOUT ANY WARRANTY OF ANY KIND, AND ALADDIN AND ITS LICENSORS HEREBY DISCLAIM ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY IN RESPECT OF THE SOFTWARE INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES AS TO NON-INFRINGEMENT. SOME STATES AND COUNTRIES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS WHICH VARY BY STATE OR COUNTRY.

5. LIMITATION OF REMEDIES. ALADDIN'S AND ITS LICENSORS ENTIRE LIABILITY UNDER, FOR BREACH OF, OR ARISING OUT OF THIS AGREEMENT, IS LIMITED TO A REFUND OF THE PURCHASE PRICE OF THE SOFTWARE OR SERVICE THAT GAVE RISE TO THE CLAIM. IN NO EVENT SHALL ALADDIN OR ITS LICENSORS BE LIABLE FOR YOUR COST OF PROCURING SUBSTITUTE GOODS. IN NO EVENT WILL ALADDIN OR ITS LICENSORS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR OTHER DAMAGES INCLUDING, WITHOUT LIMITATION, ANY LOSS OR DAMAGE TO BUSINESS EARNINGS, LOST PROFITS OR GOODWILL AND
LOST OR DAMAGED DATA OR DOCUMENTATION, SUFFERED BY ANY PERSON, ARISING FROM AND/OR RELATED
WITH AND/OR CONNECTED TO DELIVERY, INSTALLATION, USE OR PERFORMANCE OF THE SOFTWARE AND/OR
ANY COMPONENT THEREOF, WHETHER OR NOT ALADDIN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH
LOSS OR DAMAGE.

6. TERM AND TERMINATION. This license is effective until terminated. You may terminate it at any time by destroying the
Software, including all computer programs and Documentation, and erasing any copies residing on computer equipment.
This Agreement also will automatically terminate if you do not comply with any terms or conditions of this Agreement. Upon
such termination you agree to destroy the Software and Documentation and erase all copies of the Software residing on
computer equipment.

7. PROTECTION OF CONFIDENTIAL INFORMATION. The Software and Documentation are delivered to you on a
confidential basis and you are responsible for employing reasonable measures to prevent the unauthorized disclosure or use
thereof, which measures shall not be less than those measures employed by you in protecting your own proprietary
information. You may disclose the Software or Documentation to your employees as necessary for the use permitted under
this Agreement. You shall not remove any trademark, trade name, copyright notice or other proprietary notice from the
Software or Documentation.

8. OWNERSHIP. The Software and Documentation are licensed (not sold) to you. All intellectual property rights including
trademarks, service marks, patents, copyrights, trade secrets, and other proprietary rights evidenced by or embodied in or
attached/connected/related to the Software and Documentation are and will remain the property of Aladdin or its licensors,
whether or not specifically recognized or protected under local law. This License Agreement does not convey to you an
interest in or to the Software, but only a limited right of use revocable in accordance with the terms of this license agreement.
Nothing in this Agreement constitutes a waiver of Aladdin’s intellectual property rights under any law. You will not remove any
product identification, copyright notices, or other legends set forth on the Software or Documentation.

9. EXPORT RESTRICTIONS. You agree to comply with all applicable United States export control laws, and regulations, as
from time to time amended, including without limitation, the laws and regulations administered by the United States
Department of Commerce and the United States Department of State. You have been advised that the Software is subject to
the U.S. Export Administration Regulations. You shall not export, import or transfer Software contrary to U.S. or other
applicable laws, whether directly or indirectly, and will not cause, approve or otherwise facilitate others such as agents or any
third parties in doing so. You represent and agree that neither the United States Department of Commerce nor any other
federal agency has suspended, revoked or denied your export privileges. You agree not to use or transfer the Software for
end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S.
Government by regulation or specific license.

10. U.S. GOVERNMENT RIGHTS. Any Software or Documentation acquired by or on behalf of a unit or agency of the
United States Government is “commercial computer software” or “commercial computer software documentation” and,
absent a written agreement to the contrary, the Government’s rights with respect to such Software or Documentation are
limited by the terms of this Agreement, pursuant to FAR § 12.212(a) and its successor regulations and/or DFARS §
227.7202-1(a) and its successor regulations, as applicable.

11. ENTIRE AGREEMENT. This Agreement is our offer to license the Software and Documentation to you exclusively on
the terms set forth in this Agreement, and is subject to the condition that you accept these terms in their entirety. If you have
submitted (or hereafter submit) different, additional, or other alternative terms to Aladdin or any reseller or authorized dealer,
whether through a purchase order or otherwise, we object to and reject those terms. Without limiting the generality of the
foregoing, to the extent that you have submitted a purchase order for the Software, any shipment to you of the Software is
not an acceptance of your purchase order, but rather is a counteroffer subject to your acceptance of this Agreement without
any objections or modifications by you. To the extent that we are deemed to have formed a contract with you related to the
Software prior to your acceptance of this Agreement, this Agreement shall govern and shall be deemed to be a modification
of any prior terms in their entirety.

12. GENERAL. Any waiver of or modification to the terms of this Agreement will not be effective unless executed in writing
and signed by Aladdin. If any provision of this Agreement is held to be unenforceable, in whole or in part, such holding shall
not affect the validity of the other provisions of this Agreement. By entering into this Agreement, you agree to allow Aladdin to
obtain current license information from the system or systems on which the Software is installed for the purpose of
determining license renewal information. You may not assign this License Agreement or any associated transactions without
the written consent of Aladdin. This Agreement shall be construed and governed in accordance with the laws of Israel
(except for conflict of law provisions) and only the courts in Israel shall have jurisdiction in any conflict or dispute arising out
of this Agreement. The application of the United Nations Convention of Contracts for the International Sale of Goods is
expressly excluded. The failure of either party to enforce any rights granted hereunder or to take action against the other
party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of
rights or subsequent actions in the event of future breaches.
Technical Support information

Aladdin works closely with our reseller partners to offer the best worldwide Technical Support services. Your Aladdin reseller is the first line of support when you have questions about products and services; however, if you require additional assistance, contact us directly.

- For all support related issues (product overview, training, downloads and documentation, and tech support contact information), see our Web page at: www.aladdin.com/sw-support.
- To use the Aladdin KnowledgeBase, go to www.aladdin.com/kb-sw. You will need to enter your Company ID to access knowledge base articles.

Publishing history

<table>
<thead>
<tr>
<th>Date</th>
<th>Part number</th>
<th>Software release</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2010</td>
<td>76-010192</td>
<td>SafeNet MobilePASS Software Administration Guide, all versions</td>
</tr>
<tr>
<td>January 2011</td>
<td>76-010214</td>
<td>SafeNet MobilePASS Software Administration Guide, all versions</td>
</tr>
<tr>
<td>August 2011</td>
<td>007--11527-001</td>
<td>SafeNet MobilePASS Software Administration Guide, all versions</td>
</tr>
</tbody>
</table>

About SafeNet and Aladdin Knowledge Systems

In 2007, SafeNet was acquired by Vector Capital, a $2 billion private equity firm specializing in the technology sector. Vector Capital acquired Aladdin in March of 2009, and placed it under common management with SafeNet. Together, these global leading companies are the third largest information security company in the world, which brings to market integrated solutions required to solve customers’ increasing security challenges. SafeNet’s encryption technology solutions protect communications, intellectual property and digital identities for enterprises and government organizations. Aladdin’s software protection, licensing and authentication solutions protect companies’ information, assets and employees from piracy and fraud. Together, SafeNet and Aladdin have a combined history of more than 50 years of security expertise in more than 100 countries around the globe. Aladdin is expected to be fully integrated into SafeNet in the future.

For more information, visit www.safenet-inc.com or www.aladdin.com.
CHAPTER 1 MobilePASS Overview ........................................ 1
   Overview ................................................................. 2
   Deploying MobilePASS ............................................ 2
   MobilePASS authentication options ............................ 4
   Evaluating MobilePASS tokens ................................. 5

CHAPTER 2 Deploying MobilePASS .............................. 7
   Software token enrollment ...................................... 8
      Generating and importing MobilePASS software tokens ...... 8
      Configuring MobilePASS policies
         (SafeWord PremierAccess 3.2.1.06 only) ................... 8
   Assigning software tokens ..................................... 9
   Using the MobilePASS Portal ................................... 10
      Setting up manual self-enrollment for users ................... 10
      Disabling enrollment ......................................... 11
      Using the device nickname feature
         (SafeWord PremierAccess 3.2.1.06 only) .................. 12
      Using the Enrollment Portal .................................. 16
      Configuring reenrollment of existing MobilePASS tokens ... 21
   Using iPhone MobilePASS ...................................... 23
      Installing iPhone MobilePASS ................................ 23
      Activating and enrolling iPhone MobilePASS ............. 24
      Generating passcodes ......................................... 28
      Resetting the iPhone MobilePASS token .................... 28
      Changing device PINs ......................................... 29
   Understanding BlackBerry MobilePASS ..................... 31
      Deploying BlackBerry MobilePASS .......................... 31
      Authentication policy parameters .......................... 33
      Configuring automatic enrollment for BlackBerry users ... 35
   Activating MobilePASS BlackBerry ......................... 40
      Downloading and installing BlackBerry MobilePASS ...... 40
      Allowing users to automatically authenticate (SafeWord 2008 only) 40
      Activating BlackBerry MobilePASS automatically .......... 41
      Generating passcodes ......................................... 44
      Changing device PINs ......................................... 45
      Resetting the token ......................................... 46
Using J2ME MobilePASS ........................................... 47
Deploying J2ME MobilePASS .................................... 47
Downloading and installing J2ME MobilePASS ................... 47
Activating J2ME MobilePASS ................................... 48
Generating passcodes ........................................... 51
Changing device PINs .......................................... 52
Resetting the token .............................................. 53
Using Android MobilePASS ....................................... 57
Installing Android MobilePASS .................................. 57
Activating Android MobilePASS .................................. 59
Generating passcodes ........................................... 61
Changing device PINs .......................................... 63
Resetting the Android MobilePASS token ....................... 65
Getting token details ........................................... 66
MobilePASS Messaging ........................................... 67

CHAPTER 3

Using the Legacy MobilePASS Factory ....................... 69
Overview ......................................................... 70
Messaging setup .................................................. 71
The sccservers.ini file .......................................... 71
The messaging.ini file .......................................... 71
Using MobilePASS Messaging ................................... 72
Viewing Messaging end user pages ............................. 72
Using the stand-alone MobilePASS Factory .................... 73
MobilePASS Factory device compatibility ...................... 74
Using MobilePASS with SafeWord .............................. 74
Evaluating MobilePASS .......................................... 75
Installing the MobilePASS Factory .............................. 76
Downloading and installing the MobilePASS Factory ............ 76
Confirming the MobilePASS Factory installation ............... 77
Viewing and adding MobilePASS licenses ...................... 78
Viewing the current MobilePASS license ....................... 78
Adding an additional license .................................... 79
Customizing the MobilePASS Factory ......................... 81
Changing PIN behavior ......................................... 82
Finalizing custom settings ..................................... 82
Resetting token serial numbers .................................. 83
Importing token data to SafeWord .............................. 83
What’s Next? ....................................................... 84
Understanding MobilePASS packages ......................... 85
Inside the MobilePASS for Windows Desktops package ........ 85
Inside the MobilePASS for BlackBerry package ............... 85
Inside the MobilePASS for J2ME package .................... 86
Inside the MobilePASS for Smartphones package .......... 86
Inside the MobilePASS for Pocket PCs package .............. 86
Deploying the software .......................................... 87
Table of Contents

Generating batches of authenticators ........................................ 87
Using the end user authenticator download page ........................ 90
Installing MobilePASS on end user devices ............................... 91
Customizing specific device options ........................................ 92
  Customizing MobilePASS for Windows Desktops ..................... 92
  Customizing the token appearance ..................................... 92
  Customizing additional options ....................................... 92
  Customizing MobilePASS for J2ME devices ......................... 93

Index ....................................................................................... 95
CHAPTER 1

MobilePASS Overview

In this chapter...

Overview ......................................................................................... 2
MobilePASS authentication options ................................................ 4
Evaluating MobilePASS tokens........................................................ 5
Overview

This guide discusses SafeNet MobilePASS® Software and Messaging tokens. It includes administrative and end user information. Software and Messaging tokens allow users to generate OTPs (One-Time-Passcodes) on their personal mobile devices and Windows desktops. The Software and Messaging tokens are compatible with SafeWord 2008 and SafeWord PremierAccess (for Solaris), and enable secure remote access to corporate and web-based applications. An integrated support feature allows administration directly from the SafeWord management interface. The MobilePASS Portal allows users to enroll, activate, and use their tokens without administrative assistance. The MobilePASS product was integrated into SafeWord 2008 beginning in version 2.1.0.03, and in SafeWord PremierAccess (for Solaris) beginning in version 3.2.1.05.


Deploying MobilePASS

To deploy MobilePASS, administrators generate token records, populate the database with users, then notify users about MobilePASS. To generate token records, refer to the SafeWord 2008 Administration Guide, which is available at http://www3.safenet-inc.com/safeword/docs/2008.aspx or the SafeWord PremierAccess Administration Guide, version 3.2.1, which is available at http://www3.safenet-inc.com/safeword/docs/swpa.aspx. Figure 1 on page 3 illustrates the deployment process.
Chapter 1: MobilePASS Overview

Overview

Figure 1: Integrated MobilePASS deployment

1. Use SafeWord to generate and import token records with the management tools.
2. Populate database with users
3. Assign SafeWord database users passphrases through the MobilePASS Enrollment feature.
4. Provide app info and enrollment URLs to users. Give SafeWord database users enrollment passphrases.
5. Download and install MobilePASS on your device
6. Generate activation code from user device. If using auto-enrollment, enroll with an assigned passphrase.
7. Activate MobilePASS via the MobilePASS Portal.
8. Activate device, set device PIN, generate and test passcode.
9. Use MobilePASS
MobilePASS authentication options

The integrated MobilePASS product extends token options with the addition of MobilePASS Software tokens and MobilePASS Messaging tokens.

MobilePASS now allows users to generate passcodes on the following mobile devices and desktops:

- iPhone/iPod touch/iPad iOS 3.0 and higher devices
- BlackBerry OS 4.3 and higher devices
- J2ME (CLDC 1.1/MIDP 2.0 and higher) and higher devices
- Android OS 1.6 and higher devices
- Mac OS X 10.6.4 and higher
- Windows Phone version 7.0

MobilePASS Messaging’s integrated product allows users stored in Active Directory to receive passcodes in e-mail (SMTP) or text (SMS) messages directly on their desktops or mobile devices. MobilePASS Messaging is supported on Windows Server 2003 and Windows Server 2008.

Figure 2: Software Authentication Options

SafeNet’s stand-alone MobilePASS Factory is a product that includes legacy software and messaging token functionality. It is generally not advisable to use this legacy product, but it is available for configuring Messaging users in the internal SafeWord database. It also provides device-specific software token applications that work with earlier versions of BlackBerry and Windows Mobile devices, and Windows desktops. For more information about the stand-alone MobilePASS Factory software, refer to Chapter 3, Using the Legacy MobilePASS Factory Factory.
Evaluating MobilePASS tokens

SafeWord 2008 installations include four evaluation tokens (two Software and two Messaging). SafeWord PremierAccess installations include two evaluation Software tokens. The SafeWord 2008 evaluation tokens can be found in two import files (SoftwareEvalTokens.dat and MessagingEvalTokens.dat) located in the SafeWord folder, or on a new installation of SafeWord 2008, they are already present in the database. The SafeWord PremierAccess evaluation token file <Admin Console Install Dir> \SoftwareEvalTokens.dat can be imported after the SafeWord PremierAccess patch is applied. All of the evaluation Software tokens are valid tokens that can be used like any other licensed Software tokens. The evaluation Messaging tokens are intended for evaluation purposes only and should not be used in production environments. For details about the evaluation Software and Messaging tokens, refer to the Chapter 2 of the SafeWord 2008 Administration Guide or Chapter 4 of the SafeWord PremierAccess Administration Guide.

Note: The evaluation Software token records are included in the pool of available token records and will be assigned to users from the pool. If you do not want evaluation Software tokens assigned, delete the records from your database.
Chapter 1: MobilePASS Overview

Evaluating MobilePASS tokens
Deploying MobilePASS

In this chapter...

- Software token enrollment ................................................................. 8
- Assigning software tokens ................................................................. 9
- Using the MobilePASS Portal ............................................................ 10
- Using iPhone MobilePASS .............................................................. 23
- Understanding BlackBerry MobilePASS ......................................... 31
- Activating MobilePASS BlackBerry ................................................. 40
- Using J2ME MobilePASS ................................................................. 47
- Using Android MobilePASS ............................................................. 57
- MobilePASS Messaging ................................................................. 67
Software token enrollment


Generating and importing MobilePASS software tokens

Before enrolling MobilePASS tokens, the token records must be generated. The method for generating MobilePASS records varies depending upon whether you are using SafeWord 2008 or SafeWord PremierAccess. If you are using SafeWord 2008, refer to the SafeWord 2008 Administration Guide for details. If you are using SafeWord PremierAccess, refer to the SafeWord PremierAccess Administration Guide for details.

Configuring MobilePASS policies (SafeWord PremierAccess 3.2.1.06 only)

Before assigning MobilePASS tokens to users, or allowing users to self-enroll, you must configure one or more MobilePASS policies. MobilePASS policies communicate the specific capabilities of a token device between the MobilePASS clients and the portals and servers. Token capabilities are based on the device token type, (event synchronous, time synchronous, or challenge response). Some types allow you to set a minimum of policy options, while others provide an array of options, including passcode and challenge lengths, time sync interval (ticks), allow policy downgrade, secure mode, enable transaction signing mode, SoftPIN, and device PIN options.

SafeWord PremierAccess version 3.2.1.06 supports MobilePASS policies. MobilePASS policies are not supported in earlier versions of SafeWord PremierAccess or in SafeWord 2008 at this time. For details about defining policies for SafeWord PremierAccess, refer to Chapter 4 of the SafeWord PremierAccess Administration Guide.
Assigning software tokens

You may assign software tokens to users using the Administration Console, or you may allow users to self-enroll their software tokens using the MobilePASS Portal. If users will enroll their tokens with the Portal, refer to “Using the MobilePASS Portal” on page 10 of this guide.

If you are assigning software tokens to users with the Administration Console, enrollment varies slightly depending on which operating system you are using, and where your users are stored.

• If you are using SafeWord 2008, and your users are stored in Active Directory, refer to Chapter 3 of the SafeWord 2008 Administration Guide for details.

• If you are using SafeWord 2008, and your users are stored in the SafeWord database, refer to Chapter 8 of the SafeWord 2008 Administration Guide for details.

• If you are using SafeWord PremierAccess, refer to Chapter 4 of the SafeWord PremierAccess Administration Guide for details.
Using the MobilePASS Portal

The MobilePASS Portal and its Enrollment Portal provide end users with a convenient interface for enrolling software tokens without the aid of an administrator. For organizations with a large number of users, self-enrollment lightens the administrative effort when assigning tokens to users.

Users enroll their tokens using the MobilePASS Enrollment Portal, choosing either manual or automatic activation. Once tokens are enrolled, users can request token passcodes from their device, and use them to log into resources protected by SafeWord.

**Note:** MobilePASS Messaging allows users with Messaging tokens assigned to them to request passcodes be sent to them via e-mail or SMS. The passcodes can be used to log into resources protected by SafeWord. Refer to the SafeWord 2008 Administration Guide for details about Messaging tokens.

Setting up manual self-enrollment for users

When users manually self-enroll, they must first authenticate using their network credentials, or their user name and the enrollment passphrase supplied to them by their administrator. To allow users to manually self-enroll their software tokens, do the following:

1. Confirm the users are stored in the Active Directory database or in the internal SafeWord database.

   **Note:** If a user is stored in both the Active Directory and the SafeWord database, the Portal can only be used for one database or the other. You cannot use the Portal to enroll a user from both databases.

2. Ensure that there are sufficient software token records available for each user who will be self-enrolling. (Refer to the SafeWord 2008 Administration Guide or the SafeWord PremierAccess Administration Guide for more information about generating MobilePASS tokens.)

3. Ensure that the appropriate token types and policies are being used. (For SafeWord PremierAccess 3.2.1.06 only.)

4. Confirm the user has a MobilePASS enrollment reservation.

5. Provide users with the following:
   - The URL of the MobilePASS application download site, and instructions from this guide for installing MobilePASS on their device.
   - The URL for the MobilePASS Portal: https://<servername:port>/portal/enroll. By default, port 5444 is used.
   - Instructions for using the MobilePASS Portal. See “Using the Enrollment Portal” on page 16.
Disabling enrollment

You may choose to disable the software token enrollment feature entirely, or you can disable the manual feature, leaving automatic activation enabled.

To disable software token enrollment:

1. Locate the `smswebapp.ini` file. It can be found at `<tomcat_install_dir>/webapps/portal/WEB-INF/conf` (SafeWord PremierAccess 3.2.1.06), or `<install_dir>\SERVERS\Web\messaging\wepapps\portal\WEB-INF\conf` (SafeWord 2008).
2. Open the `smswebapp.ini` file using your preferred text editor.
3. Locate the following line: `DisableSoftwareTokenEnrollment`. When this line is disabled, all software token enrollment is disabled.
4. Change the setting at the end of the line to `true`.
5. Save and close the file.
6. Restart the MobilePASS Portal using the Microsoft Services tool for SafeWord 2008 installations, or restart the Tomcat server for SafeWord PremierAccess 3.2.1.06 installations.

To disable manual activation (SafeWord PremierAccess only):

1. Locate the `smswebapp.ini` file. It can be found at `<tomcat_install_dir>/webapps/portal/WEB-INF/conf`.
2. Open the `smswebapp.ini` file using your preferred text editor.
3. Locate the following line: `DisableManualEnrollment`. When this line is disabled, only manual enrollment is disabled; automatic enrollment will remain enabled.
4. Change the setting at the end of the line to `true`.
5. Save and close the file.
6. Restart the MobilePASS Portal using the Microsoft Services tool for SafeWord 2008 installations, or restart the Tomcat server for SafeWord PremierAccess 3.2.1.06 installations.
Using the device nickname feature
(SafeWord PremierAccess 3.2.1.06 only)

The MobilePASS device nickname feature allows administrators and users to assign names to their assigned token devices. Nicknames make it easier for administrators to distinguish tokens for troubleshooting when a single user has multiple MobilePASS tokens assigned to them, (for example, a BlackBerry, an iPhone and an iPad). By default, the device nickname feature is not enabled. Administrators configure it by editing lines in the Admin Console’s client.ini and/or the MobilePASS Portal’s smswebapp.ini files prior to MobilePASS token enrollment.

Note: The device nickname feature is global, and applies to all future MobilePASS enrollments until the feature is set to false.

Configuring the Admin Console to collect device nicknames

1. Open the Administration Console’s client.ini file using your preferred text editor. The file is located at <install_dir>/PremierAccess/AdminConsole.

2. Edit the CollectTokenNickname parameter in the client.ini file to match the following:
   CollectTokenNickname=true.

3. When the feature has been set to true, save and close the file.

4. Close and restart the Administration Console.


Configuring the MobilePASS Portal to collect device nicknames

1. Open the MobilePASS Portal’s smswebapp.ini file using your preferred text editor. The file is located at <tomcat_install_dir>/webapps/portal/WEB-INF/conf.

2. Add the following line or edit it to the match the following:
   CollectTokenNickname=true.

3. When the feature has been set to true, save and close the file.

4. Restart the MobilePASS Tomcat server by locating the <tomcat_install_dir>/bin directory, issuing the ./shutdown command, and then issuing the ./startup command.

5. Continue to “Collecting device nicknames (user-driven enrollment)” on page 14.
Collecting device nicknames (admin-driven enrollment)

Administrators who choose to enroll their users token devices for them, can also assign those tokens nicknames to distinguish them when multiple tokens are assigned to the same user. When configured to collect token names, these nicknames are collected and stored in the token records, providing administrators with an easy way to identify a specific token when a user has multiple tokens assigned to them. To enroll a token and specify a token nickname, do the following:

1. In the Administration Console, highlight the user name, and then select **Tools > MobilePASS Enrollment**.
2. Select **Enroll Now**.
3. Select the appropriate token policy, and then click **Next**.
4. On the device where MobilePASS is installed, start MobilePASS, choose the manual activation, and then enter the policy string that was displayed on the Administration Console wizard.

![Select Device Name](image)

5. Return to the Admin Console and select a device nickname from the predefined list, or specify your own name by selecting **Other (Please Specify)** and then click **Next**.
6. A summary screen appears. Click **Finish**.
7. Enter the Activation Code provided by the device into the field on the Administration Console, and then click **Next**.
Chapter 2: Deploying MobilePASS
Using the MobilePASS Portal

Figure 4: Actions Performed

8 Click the Finish button on the Administration Console’s MobilePASS Enrollment wizard.

9 On the token device, click the Confirm Now button.

10 Enter and reenter a device PIN, and then click Set PIN (if required).

11 A successful activation window appears on the token device along with a new passcode.

Collecting device nicknames (user-driven enrollment)

To collect devices nicknames when users self-enroll their tokens, do the following:

1 In the Administration Console, highlight the user name, and then select Tools > MobilePASS Enrollment.

2 Select User will self enroll.

3 Select the appropriate token policy, and then click Next.

4 Enter a MobilePASS Enrollment Passphrase that the user will be required to present when they enroll on the Enrollment Portal, and then click Next. The Enrollment summary window appears with the enrollment status as pending for this user.

5 Inform the user that they may now download and install MobilePASS, and enroll their token device manually. Ensure the user knows their enrollment passphrase, and the Enrollment Portal URL. Additionally, provide the user with the following information explaining how to manually enroll and name their token device.
Manually enrolling and naming a token device

To manually enroll and name a token device, do the following:

1. Download and install MobilePASS onto the token device.
2. Open MobilePASS.
3. Click the Activate Now button.
4. Click the Manual Activation button.
5. Open a browser and navigate to the MobilePASS Enrollment Portal. The Portal is located at https://<IP address or FQDN of the machine where the MobilePASS Portal is installed>:5444/portal/enroll. (The default port is 5444.)
6. Enter a user ID and the enrollment passphase as provided by the administrator.
7. Click the Authenticate button. The Software Token Enrollment window appears with a policy string and the option to select a device nickname.

**Figure 5:** Software Token Enrollment window

8. Return to the MobilePASS Activation window on the token device, and enter the Policy String from the Enrollment Portal onto the Policy field on the token device.
9. Click the Continue button. An Activation Code is displayed.
10. Enter the Activation Code displayed on the device into the Enter your activation code field on the Enrollment Portal.
11. Select a Device Name from the Select a nickname for your device list, and then click the Enroll Software Token button. A successful token enrollment window appears. You are now ready to test the token.
12. Return to the token device and click the Confirm Now button.
13. (Conditional) Enter and re-enter a Device PIN.
14 Click the **Set PIN** button. A new passcode appears.

15 Enter the passcode into the *Enter software token passcode* field on the *Enrollment Portal*, and click the **Test Software Token** button.

16 The successful test message appears. This completes enrollment.

---

**Using the Enrollment Portal**

This section describes how to use the Enrollment Portal. If users will be self-enrolling and manually activating their token, provide this information to them. If they will enroll automatically, refer to “Activating BlackBerry MobilePASS automatically” on page 41.

**Activating and enrolling software tokens manually**

To manually activate, enroll, and test tokens using the MobilePASS Enrollment Portal, do the following:

1. Install and launch *MobilePASS* on the token device. The Welcome to *MobilePASS* Activation window appears.

2. Select **Activate Now** on the device.
3 Select **Manual Activation** on the device.

4 Open a browser and go to the SafeWord Enrollment Portal at [https://<servername:port>/portal/enroll](https://<servername:port>/portal/enroll). By default, the Enrollment Portal listens on port 5444. The SafeWord Pre-authentication window appears.

**Important:** The MobilePASS Enrollment Portal requires that Internet Explorer Active Scripting is enabled in order to render the Web pages.

**Note:** You will use your Windows credentials or your SafeWord user ID and passphrase depending upon how SafeWord is set up.
5 Enter your Windows credentials or your SafeWord user ID and passphrase, and click **Authenticate**. The Activation Code window appears on the Portal. A policy string in blue text displays at the end of the first line of text on the window.

*Note: Policy-enforced authentication is not supported in SafeWord 2008.*

![Policy window](image)

6 If your device supports policy string entries, enter the **Policy String** that displays on the Token Enrollment window into the Policy field on the device, and then click **Continue**. If your device does not support policy string entry, click the **Continue** button on the device. A MobilePASS Activation Code appears on the device.

![Enter Activation Code window](image)

7 Enter the **Activation Code** from the device into the Enter your activation code field on the Enrollment Portal window, select a nickname for your device (optional), and then click the **Enroll Software Token** button.
8 (Conditional) If your administrator chose to enforce SoftPINs, the Select a software PIN (SoftPIN) window appears on the Enrollment Portal. Continue to the next step. If SoftPINs are not enforced, skip to step 11 on page 19.

Figure 11: Enter a software PIN window

9 (Conditional) Enter a SoftPIN in the Enter your PIN field, and then re-enter it in the Re-enter your PIN field. This SoftPIN must be appended to the end of the MobilePASS passcode each time you authenticate.

10 Click the Enroll Software Token button. The Test Software Token window appears with a successful enrollment message.

Figure 12: Test Token window

11 Leave this window open, return to the device, and then click the Confirm Activation button. If your administrator has chosen to enforce device PINs, the Set Device PIN window appears on the device. Continue to the next step. If device PINs are not enforced, a successful enrollment message appears along with a passcode. Skip to step 13 on page 20.
Chapter 2: Deploying MobilePASS
Using the MobilePASS Portal

Figure 13: Enter Device PIN window

12 (Conditional) Enter and re-enter a device PIN, and then click the Set PIN button.

Figure 14: Time-sync Token with Passcode

13 On the Enrollment Portal, enter the Passcode from the device into the Enter software token passcode field. If you are required to use a SoftPIN, append your SoftPIN to the end of the passcode.

14 Click the Test Software Token button. The Successful Enrollment Test window appears.
This completes the enrollment process.

If your token test fails, the Failed Results window appears. In this case, enter a new passcode in the Enter software token passcode field, and then click the Test Software Token button again. If the passcode again fails the token test, contact your administrator and request that the token be removed from your user record. Removing the token from the user record allows the user to reenroll the token.

**Note:** If the MobilePASS Enrollment Portal has been configured to allow MobilePASS users to reenroll currently-enrolled tokens, the administrator does not need to remove the token from the user’s record. The user can simply reenroll the token again. For SafeWord 2008, only Active Directory users can reenroll. To configure the Enrollment Portal for reenrollment, see “Configuring reenrollment of existing MobilePASS tokens” on page 21.

---

**Configuring reenrollment of existing MobilePASS tokens**

Administrators may choose to allow users to reenroll their MobilePASS token. Reenrollment is convenient because it eliminates the need for the administrator to unassign and reassign a token to the same user.

**Configuring reenrollment for SafeWord 2008 users (Users stored in Active Directory only)**

To allow Active Directory MobilePASS users to reenroll their software tokens without administrative assistance, a new parameter must be added to the sccservers.ini file. The parameter must be set to true. To add the parameter and the value:

1. Navigate to the `sccservers.ini` file. It can be found at `<install_dir>\SafeWord\SERVERS\Shared`.
2. Open the `sccservers.ini` file using Notepad or another text editor.
3 Scroll to the bottom of the file and add the following parameter and value:
   AllowMobilePassReEnroll=true
4 Save and close the file.
5 Restart the Admin Server. Users can now reenroll without assistance from the administrator.

Configuring reenrollment for SafeWord PremierAccess users

SafeWord PremierAccess users are stored in the SafeWord database, and can reenroll their tokens without administrative assistance if they have a maximum of one MobilePASS token assigned to them. If a user has more than one MobilePASS token assigned to them, the administrator must reenroll tokens for the user. To allow SafeWord PremierAccess users to reenroll without administrative assistance, a new parameter must be added to the
   smswebapp.ini file. The parameter must be set to true. To add the parameter, do the following:

1 Locate the smswebapp.ini file. It can be found at <tomcat install directory>/webapps/portal/WEB-INF/conf.
2 Open the file using your preferred text editor.
3 Add or edit the following line to the file:
   AllowedToReenroll=true
4 If MaxMPTokensAllowed exists, ensure that it is set to 1.
5 Save and close the file.
6 Restart the Tomcat server for the MobilePASS Portal. Users can now reenroll without assistance from the administrator. Ensure that there is a MobilePASS enrollment reservation available for the user.

Note: When a token is reenrolled, the original serial number is retained.
Using iPhone MobilePASS

iPhone MobilePASS allows users to generate passcodes directly on their iPhones, iPod touch devices, and iPads. MobilePASS is compatible with devices running iOS 3.0 or higher.

If the administrator will install MobilePASS on the device, proceed to the next section “Installing iPhone MobilePASS” on page 23.

If the end user will install and enroll their own software token, provide the user with the following:

- URL for the Apple App Store to download the MobilePASS application: http://itunes.apple.com/app/safenet-mobilepass/id364682261?mt=8
- URL for the MobilePASS Enrollment Portal: https://<servername:port>/portal/enroll
- MobilePASS installation and Enrollment Portal information.
- Credentials the user will use when activating on the Enrollment Portal (can be user’s Windows credentials or their SafeWord domain credentials).

Before generating passcodes on their iPhone/iPod touch/iPad devices, instruct users to do the following:

- Download and install the MobilePASS application to the device
- Generate a MobilePASS activation code
- Activate MobilePASS using the Enrollment Portal
- Confirm the activation and set a device PIN on the device

Installing iPhone MobilePASS

The iPhone MobilePASS application is available for download from the Apple App Store at http://itunes.apple.com/app/safenet-mobilepass/id364682261?mt=8. Download and install MobilePASS to your device following your device manufacturer’s instructions.
Activating and enrolling iPhone MobilePASS

Once installation is complete, you must activate iPhone MobilePASS. You can activate iPhone MobilePASS on the device. When you activate your iPhone MobilePASS, you enroll the token, and enable software.

**Note:** You must complete the activation process or you will continue to be prompted to complete activation each time you launch MobilePASS.

To activate and enroll iPhone MobilePASS, do the following:

1. Open the MobilePASS application on your device.

   ![Figure 16: Welcome to MobilePASS window](image)

2. Tap **Activate Now**.

   ![Figure 17: Activation Code on Device window](image)

3. The Activation Code window appears with your 20-digit activation code. Copy the **Activation Code**.

4. Open a browser and navigate to the [MobilePASS Enrollment Portal](#) using the URL provided by your administrator.

5. Log in and select **Authenticate**. The Activation Code window appears.
Chapter 2: Deploying MobilePASS

Using iPhone MobilePASS

Figure 18: Enter Activation Code on Enrollment Portal window

SafeWord Software Token Enrollment

If your software token supports policy string entry, enter this number: 9346
Otherwise ignore this information and continue with activation.

Please enter the activation code provided by your software token to continue enrollment.

![Activation Code Field]

6 Enter the activation code from MobilePASS into the Activation Code field on the Enrollment Portal, and then click **Enroll Software Token**. If your device does not support policy strings, ignore the policy string that displays. The Test Token window appears indicating successful enrollment.

7 Return to the iPhone MobilePASS application, and click the **Confirm Activation** button.

8 You are asked if you want to continue with the MobilePASS activation. Click **Yes**. The Set Device PIN window appears.

Figure 19: Set Device PIN window

![Set Device PIN Window]

9 Enter a **device PIN**, and then reenter it. The Successful Activation window appears displaying your first passcode.
10 Enter the passcode from the device into the Enter software token passcode field on the Enrollment Portal, and then click **Test Software Token**. The successful token enrollment window appears.

This completes the token enrollment.
If MobilePASS was closed before completing activation

If MobilePASS was closed before confirming activation on the device, when the device is opened again, a confirmation message appears requesting the completion of activation. In that case, do the following:

1. If you completed the activation with the previously-displayed activation code, select **Yes, activation complete**, and then skip to step 4. If you did not complete the activation, tap **No, restart activation**. The Activation Code window appears with a new activation code.

2. Enter the activation code from the device into the Activation Code field on the Enrollment Portal, and then click **Enroll Software Token**. The Test Token window appears indicating successful enrollment.

3. Return to the iPhone MobilePASS application, and click the **Confirm Activation** button.

4. You are asked if you want to continue with the MobilePASS activation. Click **Yes**. The Set Device PIN window appears.

5. Enter a **device PIN**, and then reenter it. The Successful Activation window appears displaying your first passcode.

6. Enter the passcode from the device into the Enter software token passcode field on the Enrollment Portal, and then click **Test Software Token**. The successful token enrollment window appears.

This completes the token enrollment.

You have successfully activated your MobilePASS software token.
Chapter 2: Deploying MobilePASS
Using iPhone MobilePASS

Generating passcodes

To generate passcodes for authentication:

1. Open the MobilePASS application on the device.
2. Enter your device PIN. A new passcode appears.
3. Authenticate to SafeWord using this new passcode.

Resetting the iPhone MobilePASS token

There will be instances when you will need to reset your token back to its original state.

Important: Before resetting tokens, users should contact their administrator. Unless the administrator has enabled re-enrollment privileges, the user cannot re-enroll their token until the administrator removes that token from the user’s record.

To reset the token:

1. Open the iPhone MobilePASS application and enter your device PIN.
2. Tap the Information i character in the lower right corner of the screen. The MobilePASS Information window appears with MobilePASS details.
3. Select Reset Token.

Figure 24: MobilePASS Information window
4 A message indicating that you are about to reset the token appears. You will need to re-activate the token before you can use it again.

5 Select **Reset Token**. A Welcome to MobilePASS window appears.

**Important:** Unless the administrator has enabled the reenrollment feature, the user cannot reenroll their token until the administrator removes that token from the user’s record. Any previously-assigned tokens must be manually removed by the administrator before the user can reset and reactivate (enroll) them. If the token is not removed from the user’s record first, the activation will fail.

6 Return to step 2 on page 24 of the Activating and enrolling iPhone MobilePASS section, and complete the activation process.

**Important:** If you move your MobilePASS application to a different iPhone device, the token will reset to the uninitialized state, and you must reactivate the token.

---

**Changing device PINs**

To change your device PIN, ensure that the token is activated, then do the following:

1 Open the **MobilePASS** application on the device, and enter the current device PIN.

2 Tap the **Information i** character in the lower right corner of the screen. The MobilePASS Information windows appears with MobilePASS details.
Chapter 2: Deploying MobilePASS
Using iPhone MobilePASS

Figure 26: MobilePASS Information window

3 Tap Change PIN. The Change PIN window appears.
4 Enter your current device PIN. The Enter your new device PIN window appears.
5 Enter and confirm the new device PIN that you will use with the token. You have successfully reset the device PIN.

Note: The Attack-Lock feature will reset your token if you enter the wrong device PIN ten (10) times consecutively. When the token is reset, you will need to reactivate it.
Understanding BlackBerry MobilePASS

The most recent release of BlackBerry MobilePASS (beginning with SafeWord PremierAccess version 3.2.1.06) includes the option to generate passcodes using policy-enforced challenge-response (asynchronous) mode, time-synchronous mode, or event-synchronous mode authentication on BlackBerry MobilePASS devices. These options are set in the Administration Console, with some configuration in either the .jad file or in the BES policy depending upon the kind of deployment that will be used. BlackBerry MobilePASS can be downloaded and installed directly to devices running BlackBerry OS version 4.3 and higher. The sections that follow describe how to configure and deploy MobilePASS BlackBerry.

Note: Policy-enforced authentication is not supported in SafeWord 2008.

Deploying BlackBerry MobilePASS

BlackBerry MobilePASS software tokens can be deployed:

- OTA (over the air) via the SafeNet-hosted server
- OTA via your own internally-hosted server (providing for version control)
- Via the BlackBerry Desktop Manager

Note: The BES policy configuration is not available when deploying with Desktop Manager.

- Via BlackBerry Enterprise Server (BES) application push.

The MobilePASS application is available at http://www.safenet-inc.com/GetMP. There are folders for OTA, Desktop and BES deployments. Each folder contains some combination of the following files:

- MobilePASS.cod
- MobilePASS.jad
- MobilePASS.alx.

To distribute BlackBerry MobilePASS, do the following:

1. Determine how BlackBerry device users will download the application to their device.

2. Determine if challenge-response mode, time-synchronous, or event-synchronous mode will be used. Before choosing a token type (a mode), confirm that the user’s device supports that mode.
Note: Administrators select the type of token (time-synchronous, event-synchronous, or challenge-response) using the SafeWord Administration Console. For more information about using the Administration Console, refer to the SafeWord 2008 Administration Guide or the SafeWord PremierAccess Administration Guide.

3 Configure the appropriate policies for challenge-response, time-synchronous, or event-synchronous mode (see “Configuring MobilePASS policies (SafeWord PremierAccess 3.2.1.06 only)” on page 8).

4 Post the appropriate files, based on the download method, to a location where users can access them, and then do the following:
   - Inform the user of the location where the software is available for downloading and installing.
   - Inform the user that they must set a device PIN the first time they launch BlackBerry MobilePASS on their device. (Conditional)

Note: Administrators may also install the BlackBerry MobilePASS software onto the device, and then distribute the device to the user. This method is convenient when there are a small number of users.

Important: If users upgrade to the most recent version of MobilePASS, the BlackBerry client will prompt for a device PIN after the upgrade. To resolve this issue for devices that do not support device PINs, uninstall MobilePASS from the device, reinstall it, and then reactivate the token.


**Authentication policy parameters**

BlackBerry MobilePASS authentication policy parameters are set in the .jad file for OTA deployments, and in the BES policy for BES deployments. By default, the authentication policy parameter values are as follows:

- DisableSafeNetMobilePASSPolicy = False
- EnforceSafeNetMobilePASSPolicy = False

Table 1 describes each parameter, its key values, and functions.

**Table 1: BlackBerry authentication policy parameters, value options and functions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Key value(s)</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>DisableSafeNetMobilePASSPolicy (if policy strings are not supported by backend server, the client does not prompt for policy)</td>
<td>• True • False</td>
<td>Specifies the authentication mode, either legacy event-synchronous, policy-enforced event-synchronous, time-synchronous, or challenge-response.</td>
</tr>
<tr>
<td>EnforceSafeNetMobilePASSPolicy</td>
<td>• True • False</td>
<td>Specifies that authentication will be policy enabled, and whether or not the policy field can be left blank.</td>
</tr>
</tbody>
</table>

**Configuring authentication policies via the .jad file**

To configure the authentication policy in the .jad file, do the following:

1. On the machine where the BlackBerry MobilePASS application is located, navigate to the .jad file.
2. Open the .jad file with a text editor such as Notepad.
3. Add the Authentication Policy Parameters with the desired values to the .jad file (refer to Table 1 on page 33).
4. Save and close the file.
Configuring authentication policies via the BES policy

To configure the authentication policy via the BES policy, do the following:

1. Open the BlackBerry Administration Console and log in to the BES.

   **Important:** All BES IT policy rules used by MobilePASS must be created using type String. Some MobilePASS rules are Boolean in nature. However, these IT policy rules must be created using type String, and not type Boolean. Valid string representations of Boolean values are `false`, `disabled`, `disable`, `no`, `0`, `true`, `enabled`, `enable`, `yes`, `1`. Failure to use type String will result in policy rules reverting to default values.

2. Expand the Policy node in the BlackBerry solution management pane, and select your IT policy rule. If you have not created an IT policy, create one using the information contained in “Configuring BlackBerry auto-enrollment via the BES policy” on page 37.

3. When the policy has been edited with the authentication policy parameters, save the configuration, log out, and close the BlackBerry Admin Console.
Configuring automatic enrollment for BlackBerry users

The latest version of BlackBerry MobilePASS can be configured to allow users to automatically self-enroll their tokens OTA via the MobilePASS Portal. This feature is available beginning with SafeWord 2008, version 2.1.0.04 and SafeWord PremierAccess, version 3.2.1.05.

By default, auto-enrollment is pre-configured, and can be used right away using the .jad file. Please see “BlackBerry auto-enrollment parameters” on page 35 for the .jad files’ default parameter values. If you want to customize the parameters of the .jad file to meet your organization’s needs, you must add the parameters described in Table 2 on page 36, along with the appropriate values for the parameters. For BES deployment, you must update or create a policy for auto-enrollment.

If you will be editing the .jad file, refer to “BlackBerry auto-enrollment parameters” on page 35. If you will be creating a policy for auto-enrollment in the BES policy, refer to “Configuring BlackBerry auto-enrollment via the BES policy” on page 37.

BlackBerry auto-enrollment parameters

These parameters can be used either in the .jad file, or set via BES policy to customize your users auto-enrollment experience.

Note: By default, if no parameters are added, the user will be prompted to either manually or automatically enroll.

The following is a list of auto enrollment parameters. The default parameter value is indicated by bold text.

- SafeNetMobilePassActivationMethod: Prompt
- SafeNetMobilePassActivationURL:
- SafeNetMobilePassModifyURL: true
- SafeNetMobilePassActivationFailover: true

Important: The default mode values will be used by the MobilePASS client if no other values pairs are specified in the .jad file or in the BES policy.
Table 2 on page 36 describes the parameters, including key values, and functions. Use this information to configure auto-enrollment.

**Table 2**: BlackBerry auto-enrollment parameters, value options, and functions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Key value(s)</th>
<th>Function</th>
</tr>
</thead>
</table>
| SafeNetMobilePASSActivation-Method | • Manual  
• Automatic  
• Prompt                              | Specifies the activation method, either manual enrollment, automatic enrollment, or the user will be prompted for method.                        |
| SafeNetMobilePASSActivationURL   | Valid https URL or null if none     | Specifies the MobilePASS Portal URL.                                                                                                                     |
| SafeNetMobilePASSModifyURL       | • True  
• False                                | Allows the user to view and modify the auto enrollment URL in the device UI.                                                                            |
| SafeNetMobilePASSActivation-Failover | • True  
• False                                | Allows failover to manual enrollment if auto enrollment fails. True presents user with the option to manually enroll in addition to retrying auto enrollment.|

**Configuring BlackBerry auto-enrollment via the .jad file**

To configure automatic enrollment by editing the parameters in the .jad file, do the following:

1. On the machine where the BlackBerry MobilePASS application is located, navigate to the .jad file.
2. Open the .jad file with a text editor such as Notepad.
3. Add the **Auto-enrollment Parameters** with the desired values to the .jad file (refer to Table 2 on page 36).
4. Save and close the file. Users can now auto-enroll their BlackBerry tokens.
Configuring BlackBerry auto-enrollment via the BES policy

To configure automatic enrollment by editing the BES policy, do the following:

1. Open the BlackBerry Administration Console and log in to the BES.
2. Expand the Policy node in the BlackBerry solution management pane, and then select Create an IT Policy.

3. (Optional) Enter a name for the policy in the Name field, and then click the Save button.
4. From the BlackBerry solution management pane, select Create an IT policy rule.

5. Add a new rule to the IT policy by entering the name SafeNetMobilePassActivationURL in the Name field, selecting String from the Type menu, selecting Handheld from the Destination menu, and then clicking Save.

   **Note:** Additional parameters from Table 2 on page 36 may be added to the policy based upon your organization’s preferences.

6. From the BlackBerry solution management pane, select Manage IT Policies.
Figure 29: Manage IT policies window

7 Select the policy that was created in step 5 on page 37.

Figure 30: Edit IT policy option

8 From the menu, select the **Edit IT policy** option.

Figure 31: User defined tab

9 Select the **User defined** tab.
10 Set the SafeNetMobilePassActivationURL value to the **URL of the MobilePASS Portal**.
Activating MobilePASS BlackBerry

### Downloading and installing BlackBerry MobilePASS

If BlackBerry MobilePASS is deployed via the BES, the BES delivers the MobilePASS application to the device automatically along with the IT policy. If you are not using BES deployment, install BlackBerry MobilePASS onto the BlackBerry device by doing the following:

**From the BlackBerry device:**

1. Launch a browser and navigate to the site where the BlackBerry MobilePASS OTA files have been posted.
2. Download and install MobilePASS.

**Using BlackBerry desktop software:**

1. Launch a browser and navigate to the site where the BlackBerry MobilePASS Desktop files have been posted.
2. Download and install MobilePASS.
3. Sync the Desktop software with the BlackBerry software.

**Tip:** If BlackBerry MobilePASS is being used on a BlackBerry Storm device, disabling the compatibility mode feature ensures the best touch-screen experience for the user.

**Important:** Keep the MobilePASS application open until activation is complete.

### Allowing users to automatically authenticate (SafeWord 2008 only)

During automatic enrollment, BES may be used to identify users to the MobilePASS Portal. This eliminates the need to provide user credentials during activation. Users simply set their device PIN (if required) and begin generating passcodes.

**Important:** Auto-authentication is only available with BES, and only supports Active Directory users.

To enable auto-authentication, the BES must be configured to add headers to HTTPs requests and the MobilePASS Portal must be configured to allow auto-authentication. The headers identify users by their email addresses. The MobilePASS Portal uses the email address to identify and authenticate users.
Activating BlackBerry MobilePASS automatically

The first time you open BlackBerry MobilePASS on the device, the Welcome to MobilePASS window appears requesting that you activate MobilePASS.

To automatically enroll a software token, do the following:

1. Download and launch **MobilePASS** on the token device. The Welcome to MobilePASS window appears.

   ![Welcome window](image)

   **Figure 33:** Welcome window

2. Select **Activate Now**. The MobilePASS Activation window appears.

   ![Activation window](image)

   **Figure 34:** MobilePASS Activation window

3. Select **Automatic Activation**. The URL window appears.

   ![URL window](image)
4 Enter the URL of the Enrollment Portal, and the port on which it listens in the following format https://<servername:port>/portal/enroll, and then click the Activate button. The User ID and Passphrase window appears.

5 Enter your user ID and the passphrase provided by your administrator, and then click Submit. The Activating window appears. When it completes, the device PIN window appears.
6 Enter and re-enter your desired device PIN, and then click the Set PIN button. The Successful Activation window appears with a passcode for use.

**Figure 37:** Device PIN window

**Figure 38:** Time Sync token with passcode window

---

**Note:** To configure automatic enrollment for BlackBerry MobilePASS users, administrators must add the necessary auto enrollment parameters into the .jad file or to their BES policy.
Generating passcodes

To generate a new MobilePASS passcode, open MobilePASS.

1 Enter your device PIN (if required), and then click Generate Passcode.

2 (Conditional) If the token is a challenge-response mode token, enter the challenge that was provided, and then click the Generate Passcode button.

3 To generate another passcode, click Generate Passcode on a non-policy token or click New Challenge on a policy-enforced token.
Changing device PINs

To change your device PIN, do the following:

1. Open BlackBerry MobilePASS.
2. Enter your device PIN. (If required)
3. Enter the Challenge. (If required)
4. Select Generate Passcode.
5. Select the BlackBerry Menu button on the device. A menu appears with the Change PIN option displayed.

![Figure 41: Change device PIN option](image)

6. Select Change PIN. The Change PIN window appears.

![Figure 42: Change device PIN window](image)

7. Enter your current device PIN, then enter and re-enter a new PIN.
8. Select Change PIN. A new window appears displaying a new passcode. The device PIN has successfully been changed.

**Note:** If you are using a token that does not support MobilePASS token policies, the Attack-Lock feature will reset your token when you enter the wrong device PIN ten (10) times consecutively. When the token is reset, you will need to reactivate it. If you are using a MobilePASS token that supports policies, the number of attempts allowed before attack lockout varies depending upon the policy being used.
Resetting the token

To reset your token to its original state, do the following:

1. Open BlackBerry MobilePASS. If your token requires a device PIN, the device PIN Challenge window appears. If your token does not require a device PIN, skip to step 4.
2. Enter your device PIN.
3. Click Generate Passcode. The window appears displaying a passcode.
4. Click the BlackBerry Menu button, and then select the About option. The About MobilePASS window appears displaying the Reset Token option.

**Important:** Before resetting tokens, users should contact their administrator. Unless the administrator has enabled reenrollment privileges, users cannot reenroll their token until the administrator removes that token from the user’s record.

5. Click Reset Token. A new window appears informing you that you are about to reset your token.
6. Click Reset Token. The Confirm Reset window appears.
7. To confirm the reset, click Yes. You must now reactivate MobilePASS. To reactivate, refer to “Activating and enrolling software tokens manually” on page 16.

**Note:** The BlackBerry MobilePASS software token will need to be re-activated each time a major release of the BlackBerry operating system is applied, since the MobilePASS data is not backed up for security reasons. The user will also need to reenroll the token, including device PIN settings at this time.
Using J2ME MobilePASS

The latest release of the integrated MobilePASS product includes J2ME MobilePASS. J2ME MobilePASS runs on select mobile devices that are enabled with Sun’s Java 2 Micro Edition Platform or Micro Edition Support (CLDC 1.1/MIDP 2.0). Once J2ME MobilePASS is installed and activated on the device, users can generate SafeWord strong authentication passcodes directly from their device.

Deploying J2ME MobilePASS

J2ME MobilePASS consists of two files, MobilePASS.jar and MobilePASS.jad. The files are contained in a zipped file. Both files should be made available for over-the-air (OTA) download via your internally-hosted server. Once the files are on your server, inform your J2ME device users that MobilePASS is available for them to use for SafeWord authentication. Provide the users with a link to the software download location.

Downloading and installing J2ME MobilePASS

To download and install J2ME MobilePASS, from the J2ME device, browse to the MobilePASS application link provided by your administrator, and then download the MobilePASS.jar and MobilePASS.jad files to your device. Use the MobilePASS.jad file to automatically install J2ME MobilePASS on your device. When the installation is complete, the SafeNet MobilePASS icon appears on your device’s main display.

Note: The location of the J2ME MobilePASS icon may vary depending upon the installation settings of your device.

Tip: Your J2ME MobilePASS screens and menu items may not match the screen shots displayed in this guide.
Chapter 2: Deploying MobilePASS

Using J2ME MobilePASS

Activating J2ME MobilePASS

The first time you open J2ME MobilePASS on the device, the Welcome to MobilePASS window appears, requesting that you activate the product.

1. To activate MobilePASS, click Next. The Activation Code window appears.

2. Click Confirm. The Confirmation window appears.

3. Use the Activation Code to enroll the token on the Enrollment Portal by doing the following:
   a. Copy the Activation Code. A window will display
   c. Enter your network credentials or your user name and password, and then click Authenticate. The Activation Code window appears.
d Enter the 20-digit activation code that was copied from the device.

e Click **Enroll Software Token**. The Test Software Token window appears.

f Return to the device. A Confirmation window appears.

Figure 47: Confirmation window with scroll bar

4 You may need to scroll down to read the entire confirmation. When you have read the confirmation, click **Yes**. The Create a device PIN window appears.

Figure 48: Create a device PIN window

5 Enter a four-digit **device PIN** in the Enter device PIN field.
Figure 49: Re-enter device PIN window

6 Highlight the Re-enter PIN field, and re-enter the same device PIN there.

7 Click Set PIN.

Figure 50: Successful Activation window

8 The Successful Activation window appears, and displays your passcode. You may use this passcode to authenticate to SafeWord. Click Close to end this session.
Generating passcodes

To generate passcodes, open MobilePASS. The Enter device PIN window appears.

1 Enter your device PIN, and then click OK.

2 Your new passcode appears.Authenticate to SafeWord using this passcode.

3 To generate another passcode, click Options. The Generate Next option appears.
4 Click **Generate Next**. A new passcode appears for use.

### Changing device PINs

To change your device PIN, do the following:

1. Open **MobilePASS**.
2. Enter your device PIN, and then click **OK**. The Passcode window appears.

3. Select **Options**, highlight **Change PIN**, then click **OK**. The Change device PIN window appears.
4 Enter your current device PIN in the Enter current device PIN field.
5 Highlight the Enter PIN field, and enter a new device PIN.
6 Highlight the Re-enter PIN field, and re-enter the new device PIN.
7 Click OK. A new passcode appears, and your device PIN has been changed.

**Note:** The Attack-Lock feature will reset your token if you enter the wrong device PIN ten (10) times consecutively. When the token is reset, you will need to reactivate it.

---

### Resetting the token

**Important:** Before resetting tokens, users should contact their administrator. Unless the administrator has enabled re-enrollment privileges, the user cannot re-enroll their token until the administrator removes that token from the user’s record.

To reset your token back to its original state, do the following:

1 Open MobilePASS.
2 Enter your device PIN.
3 Click OK. A passcode appears.
4 Click **Options > About**, and then click **OK**. The About MobilePASS window appears.

5 Select **Reset Token**. A new window appears informing you that you are about to reset your token.
Figure 58: Reset window

6 Select Reset. The Confirm Reset window appears.

Figure 59: Confirm Reset window

7 Click Options. Reset No and Yes options appear.
Figure 60: Select Yes window

8 Highlight Yes, and then click OK. You are returned to the Activation window.

Figure 61: Activation window

9 Click Next, and then reactivate MobilePASS. If you need assistance, refer to “Activating J2ME MobilePASS” on page 48.
Google Android is the latest mobile device for which the MobilePASS product is available. MobilePASS Android users can generate one-time-use passcodes directly on their Android mobile device, and use those passcodes to authenticate to SafeWord-protected applications and resources. Android MobilePASS is compatible with Google Android versions 1.6 and 2.x.

Installing Android MobilePASS

To install Android MobilePASS:

1. Start the Android Market application by clicking or touching the Market icon on the Android Gallery. The Market appears displaying the applications that are available.

![Android Market](image)

2. Enter MobilePASS in the Search field, and then select the Search icon.

![Search for MobilePASS](image)

The MobilePASS application appears for downloading.

3. Click or tap the MobilePASS icon.

4. Click or tap the Install button.
5 Click or tap OK. The download begins.

When the download is complete, the MobilePASS icon appears on the Android Gallery (Figure 65).

6 To activate MobilePASS, click or tap the **MobilePASS** icon. The Welcome to MobilePASS window appears.

7 Click or tap **Activate Now** to begin the activation. Continue to the next section, “Activating Android MobilePASS” on page 59.
Activating Android MobilePASS

The first time you open Android MobilePASS on the device, the Welcome to MobilePASS window appears (see Figure 66 on page 58). To activate the application, click the Activate Now button. The Activation Code window appears. Use the activation code to enroll the token on the Enrollment Portal by doing the following:

1. Copy the Activation Code. A window will display.
3. Enter your network credentials or your user name and password, and then click Authenticate. The Activation Code window appears.
4. Enter the 20-digit activation code that was copied from the device.
5. Click Enroll Software Token. The Test Software Token window appears.
6. Return to the device.

Important: If you close MobilePASS before confirming the activation, the Incomplete Activation Alert window appears. Click or tap No, restart activation, and continue to the next step.

On the Activation Code window, click or tap the Confirm Activation button. The Set device PIN - Enter New device PIN window appears.

Figure 67: Activation Code window

Figure 68: Set device PIN - Enter New device PIN window
8 Enter a device PIN to use with this token, and then click or tap OK. The Re-Enter PIN window appears.

![Figure 69: Re-Enter device PIN window](image)

9 Confirm the device PIN by re-entering it. Click or tap OK. A new passcode appears with the message that you have successfully activated MobilePASS.

![Figure 70: Successful Activation window](image)

10 To generate another passcode, click or tap the Generate Passcode button.
Generating passcodes

To generate passcodes:

1. Open Android MobilePASS. If your token requests a device PIN, the device PIN challenge window appears.

   ![Figure 71: Enter your device PIN window](image)

2. Enter your device PIN.
   
   a. If the correct device PIN was entered, the Passcode appears. Continue to the next numbered step.
   
   b. If the wrong device PIN was entered, the Incorrect device PIN window appears (see Figure 73 on page 62). Skip to step 4 on page 62.

   ![Figure 72: Passcode window](image)

3. Authenticate to SafeWord using this passcode.
Figure 73: Incorrect device PIN window

4 Click or tap OK. The Enter your device PIN appears. This window includes the number of attempts you have made to enter your device PIN. If you do not enter the correct device PIN in 10 attempts, the Attack Lock feature will force you to reset the token.

*Note:* When the Attack Lock feature forces you to reset a token, the token must be reactivated.

Figure 74: Attempted device PIN window

5 Enter your device PIN, and then click or tap OK. A new passcode appears.
Changing device PINs

If you want to change your device PIN, do the following:

1. Open MobilePASS. The Enter your device PIN window appears.
2. Enter your device PIN, and click or tap the OK button.
3. Click or tap Generate Passcode.
4. Select the Android Menu button on the device.

*Note: If you hold the Menu button for more than two seconds, the window changes from that of View A below to View B.*

5. On the Options window, click or tap Advanced Options. A new window appears with the Change PIN option displayed.

6. Click or tap Change PIN. The Change device PIN window appears.
7 To change the current device PIN:

a Enter the current **device PIN** that is associated with this token in the Enter Current PIN window, and then click or tap **OK**.

b Enter a new device PIN in the Enter New PIN window, and then click or tap the **Change PIN** button.

c Re-enter the new device PIN in the Enter New PIN window, and then click or tap the **Change PIN** button. The Successful PIN change window appears.

8 Click or tap **OK**.
Resetting the Android MobilePASS token

**Important:** Before resetting tokens, users should contact their administrator. Unless the administrator has enabled re-enrollment privileges, the user cannot re-enroll their token until the administrator removes that token from the user’s record.

To reset your token back to its original state, do the following:

1. Open Android MobilePASS. If your token requires a device PIN, enter the device PIN at the challenge. A Passcode appears.
2. Select the Android **Menu** button on the device. The Options window appears.
3. Select the **Advanced Options** button. A new window appears with the Reset Token option displayed.
4. Click or tap **Reset Token**. The Activation Code window appears.
5. Reactivate the token using the instructions provided in “Activating Android MobilePASS” on page 59.
You have successfully re-activated your MobilePASS software token.

### Getting token details

To view the token details:

1. Open **MobilePASS Android**.
2. Click or tap the Android **Menu** button on the device, and then click or tap the **About MobilePASS** option. Details about the token appear.
3. Click or tap **Done** to close the window.
The MobilePASS Messaging application is the component of SafeWord MobilePASS that allows users to request and receive authentication passcodes via e-mail (SMTP) and text messages (SMS) directly on their desktop or on their mobile device. The Messaging application is supported on Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2 operating systems. For more information about configuring MobilePASS Messaging, refer to the MobilePASS Messaging section in the SafeWord 2008 Administration Guide.
In this chapter...

Overview ................................................................. 70
Messaging setup ............................................................. 71
Using MobilePASS Messaging ........................................ 72
Using the stand-alone MobilePASS Factory ......................... 73
Installing the MobilePASS Factory .................................... 76
Viewing and adding MobilePASS licenses .......................... 78
Customizing the MobilePASS Factory ............................... 81
Resetting token serial numbers ........................................ 83
Importing token data to SafeWord ..................................... 83
What’s Next? .................................................................. 84
Understanding MobilePASS packages ............................... 85
Deploying the software ................................................... 87
Installing MobilePASS on end user devices ....................... 91
Customizing specific device options ................................. 92
SafeNet recommends that you use the latest version of MobilePASS that is integrated with SafeWord 2008 and SafeWord PremierAccess. The earlier legacy version described in this chapter offers support for MobilePASS clients on older versions of BlackBerry and Windows Mobile (up to 6.x) devices. It also allows Messaging use for users in the SafeWord user database. If you do not have these needs, please skip this chapter, and use the current version of MobilePASS. If you choose to use the earlier version, the following information describes how to use the stand-alone MobilePASS Factory. The MobilePASS Factory allows you generate records for the authenticator type called **Messaging**, that uses SMS or SMTP to provide authenticating passwords to users’ mobile devices. Before these authenticators can be assigned to your users, you will need to generate them using MobilePASS Factory and then import them into your SafeWord installation (see “Importing token data to SafeWord” on page 83).

Once the authenticators have been imported, a user’s MobilePASS routing information can be set up in the stand-alone Management Console (Admin Console). This is done by selecting the MobilePASS authenticator you want to edit (Find > Authenticators > Software/Hardware Authenticators), calling up its **Edit Hardware Authenticator** window, and selecting **MobilePASS Route** in the **Additional Options** menu (if needed, refer to the **SafeWord 2008 Administration Guide** for more information). The blank field should contain one of the following:

- **If using SMTP**: the user’s email address
- **If using SMS**: the user’s cell phone number

This field can also be populated by the user during the authenticator generation step in the MobilePASS Factory.

**Note:** *This option is not available if you generate a batch of authenticators.*
**Messaging setup**

The core messaging servlet is installed with the MobilePASS Factory, however there are a few items that need to be configured before you can use it.

---

### The sccservers.ini file

If your users reside in the SafeWord database instead of Active Directory, add the following line to the sccservers.ini file (found in `<Install_Dir>/SERVERS/Shared` directory):

```ini
userDBType=securecomputing.nbt.tokens plugin.SWUserDBMapper
```

---

### The messaging.ini file

The file `../MobilePass/data/config/messaging.ini` must be configured for the messaging provider to determine if it’s using SMS or SMTP. You will also need to configure the SafeWord Administration Server that will be used to get the routing information for password delivery as well as get the user’s password. The file `messaging.ini` has comments that explain the various required settings, as well as parameters to control where the user will be redirected after the password has been sent.
Using MobilePASS Messaging

When a user needs a password, they use the browser on their cell phone or PC to connect to the appropriate URL to request a password.

The URL will be something similar to:

https://hostname:5443/MPapp

The web page will prompt the user for their name, then deliver the password after the page is submitted. If using a cell phone, it may be convenient to store a link with all the necessary parameters so that, when a password is needed, the user only has to select the link or icon on their phone and there will be no other data entry required. Below is an example link:

https://hostname:5443/MPapp/PasswordRequest.do?name=joe

**Note:** In the example above, *joe* would be replaced by an actual user’s name.

This could also be stored as a bookmark in the user's PC browser.

**Viewing Messaging end user pages**

You can view the pages your end users will see when requesting either an authenticator or password in the MPF by selecting View the Messaging end user authenticator request page, or View the Messaging end user password request page.

**Figure 83:** Messaging end user pages
Using the stand-alone MobilePASS Factory

The stand-alone MobilePASS Factory can be installed either on the same machine as SafeWord, or on a different machine. After installation, the stand-alone MobilePASS can be customized to fit your organization’s needs and generate platform-specific packages.

You will import token records into SafeWord and assign authenticators to users. Users are notified that they may authenticate using MobilePASS, and they obtain their relevant package(s). After installing MobilePASS on their device, your users can begin authenticating using MobilePASS-generated passcodes. Figure 84 shows the token deployment process using the stand-alone MobilePASS management feature.

**Figure 84:** Stand-alone MobilePASS deployment
MobilePASS Factory device compatibility

MobilePASS is compatible with a wide variety of devices and platforms:

- MobilePASS for BlackBerry running RIM BlackBerry version 3.8 operating systems
- MobilePASS for J2ME devices enabled with Sun’s Java 2 Micro Edition Platform or Micro Edition Support (CLDC 1.1/MIDP 2.0)
- MobilePASS for Pocket PCs running Windows Mobile 5.0 or later
- MobilePASS for Smartphones running Windows Mobile 5.0 or later

MobilePASS can be installed using each device’s standard installation processes. You simply send your end users a device-specific MobilePASS package or allow them to download their authenticator themselves. Once installed, MobilePASS is ready to generate passcodes for authentication.

Using MobilePASS with SafeWord

The following are required for using MobilePASS with SafeWord:

- Windows Platforms: SafeWord 2008 (with the core servers installed on Windows 2003/2008 servers), SafeWord Version 4.0.0.04 or later (with the core servers installed on Windows 2000 or Windows 2003 servers). On Solaris platforms, SafeWord PremierAccess Version 3.2.1 or later.

  Note: MobilePASS Factory (MPF) must be installed on Windows XP (Home or Professional), Windows 2003/2008, or Vista (32-bit or 64-bit).

- Valid SafeWord 2008 license with the Enterprise Solution Pack enabled.
- An Internet connection is recommended in order to obtain the latest updates of MobilePASS automatically.

The following component specifications are required for running the MPF:

- CPU: Pentium III @ 500 MHz or better
- RAM: 256 MB (minimum), 512 (recommended)
- Disk space: 200 MB (minimum) 2 GB (recommended)
Evaluating MobilePASS

MobilePASS ships with a license that can be used to generate five authenticators for evaluation purposes. This license automatically loads during MobilePASS startup, unless a valid user license is detected. Since these authenticators are meant for evaluation purposes only, MobilePASS generates their import records using the same key for all evaluation customers.

⚠️ **Important:** As the evaluation import records all share the same key, they should not be used in a production environment.
Installing the MobilePASS Factory

The MobilePASS Factory can be downloaded from the SafeNet Web site. After installation, the MobilePASS Factory, a standalone component, is used to generate MobilePASS device packages for end users.

**Downloading and installing the MobilePASS Factory**

To download the MobilePASS Factory, browse to [http://c3.safenet-inc.com](http://c3.safenet-inc.com). Table 3 is a checklist for downloading and installing. As noted earlier, MobilePASS can be installed on the same server where SafeWord is installed, or it can be installed on a different machine in the network.

**Table 3: Checklist for MobilePASS Installation**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Locate the SafeWord 2008 or MobilePASS serial number</td>
</tr>
<tr>
<td></td>
<td>Satisfy the requirements for using MobilePASS with SafeWord</td>
</tr>
<tr>
<td></td>
<td>Run <strong>Setup.exe</strong></td>
</tr>
</tbody>
</table>
Confirming the MobilePASS Factory installation

After installation, confirm the following:

- The MPF is available from Start > Programs > Aladdin > MobilePASS > MobilePASS Factory.

- MobilePASS configuration files (mobilepass.ini, mpdefaultparam.ini, messaging.ini, and webconfig.ini) are present in <install_dir>\MobilePass\data\config.

Tip: For support information, use the Windows Add or Remove Programs tool to locate MobilePASS in the list of currently installed programs. Select Click here for support information.
Viewing and adding MobilePASS licenses

If MobilePASS detects a valid license, the details of that license are available for viewing from the MPF, and an additional license can also be added from the MPF. To check the current license information, continue to Viewing the current MobilePASS license. If additional licenses are needed, continue to “Adding an additional license” on page 79.

Viewing the current MobilePASS license

A valid MobilePASS user license and its details can be viewed from within the MobilePASS Factory.

To view the current MobilePASS license:

1. From the Start menu, select Programs > Aladdin > MobilePASS > MobilePASS Factory.

**Figure 85: MobilePASS Factory window**

Welcome to the MobilePass Factory

From this page, you may accomplish the following:

- Generate authenticator
- View current license or add another license

You may also view end user pages:

- View the end user authenticator download page
- View the Marketing end user authenticator request page
- View the Marketing end user password request page
2 When the Welcome window appears, select **View current license or add another license**.

In Figure 86, the upper portion of the License Management window shows the current MobilePASS license information, and the lower portion provides tools for adding additional licenses. The MobilePASS license can be used for any of the supported device packages. To add an additional license, refer to Adding an additional license.

### Adding an additional license

To add an additional MobilePASS license, a MobilePASS activation certificate is needed. It contains the data for activating a new license. With that information and the activation code that was generated during MobilePASS activation:

1. Open the MobilePASS Factory by selecting **Start > Programs > Aladdin > MobilePASS > MobilePASS Factory**.

2. When the Welcome window appears, select **View current license or add another license**.

The lower portion of the window is the Add Additional License tool.
3  Enter all the requested information (from the MobilePASS activation certificate), plus the Activation Code in the **Activation Code** field.

The activation code was delivered via the Web or e-mail.

4  Click the **Add License** button.

The updated license information displays in the upper portion of MobilePASS License Management window.
Customizing the MobilePASS Factory

After installation, files are written into the `<install_dir>\MobilePass\data\config` directory that control and allow customization of MobilePASS. Microsoft Notepad or a similar text editor can be used to edit these files.

For example: you could display your own company logos, icons, names, and symbols in the MobilePASS interface, or you can customize the appearance of the Windows Desktop tokens, and require that PINs be appended to the passcodes for authentication. Table 4 and the sections below it summarize the MobilePASS configuration files, and further customizing information is included in each of the configuration files.

Table 4: MPF Configuration Files (found in `<install_dir>\MobilePass\data\config`).

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>messaging.ini</td>
<td>The config file for message delivery and user redirect.</td>
</tr>
<tr>
<td>mobilepass.ini</td>
<td>The main MPF server configuration file.</td>
</tr>
<tr>
<td>mpdefaultparam.ini</td>
<td>MPF programming parameters.</td>
</tr>
<tr>
<td>webconfig.ini</td>
<td>The file in which MPF html files are specified.</td>
</tr>
</tbody>
</table>

**Important:** These files can be renamed arbitrarily. The property names (the names to the left of the equal sign) inside the file must not be modified.

**messaging.ini**

This file contains configurations for determining whether Short Message Service (SMS) or Simple Mail Transfer Protocol (SMTP) will be used for password delivery. It includes configurations that determine which SafeWord Admin server will be used for the routing information for password delivery, and parameters to control user re-directs after password transmission.

**mobilepass.ini**

This is the main configuration file for MobilePASS. The token record output file, and the name of the configuration file containing the token programming parameters are configured here. If parameters in this file are changed, the MPF service must be restarted.

**mpdefaultparam.ini**

This is the file containing MobilePASS authenticator programming parameters. If the file name is changed, the value must also be changed in `mobilepass.ini`. All parameter values can be customized within the file using a text editor such as Microsoft Notepad. This file also includes details about parameter default settings, optional settings, and functionality. If parameters in this file are changed, the MPF service must be restarted.
Important: Specific PIN modes or other configuration parameters that affect how end users authenticate, should be conveyed to those users.

webconfig.ini

This file contains html pages that are used with MobilePASS. All aspects of these pages are customizable. Unique corporate images and icons, user messages, and user data collection fields can be displayed on these pages. The actual web pages that can be customized are located in <install_dir>/data/templates/html. If parameters in this file are changed, the MPF service must be restarted.

In addition to customizing general MobilePASS and MobilePASS Factory behavior, you can customize certain device-specific aspects of MobilePASS. These device-specific configuration options are described in “Customizing specific device options” on page 92.

Changing PIN behavior

You can add a second layer of security by requiring that a PIN be used with the passcode during user authentication. PIN behavior parameters can be set in the mpdefaultparam.ini file. The following PIN modes are available:

• Local mode: In this mode, the PIN is required in order to generate the next passcode. Hence, the user is prompted for one before a passcode can be generated (local mode is the recommended PIN mode.)

• Append mode: In this mode, PINs are used in exactly the same fashion as they would be with a hardware authenticator. A PIN would be assigned to the user’s authenticator via the SafeWord 2008 Management Console or Active Directory Users and Computers (ADUC). It would then be appended to the passcode at authentication time. With this approach, a PIN is not required in order for MobilePASS to generate a passcode.

Finalizing custom settings

To finalize custom settings:

1  Launch the Services tool by selecting Start > Programs > Administration Tools > Services.

2  Locate and highlight the MobilePASS Factory in the list of services.

3  Select Restart the service option in the upper left corner of the window.
Chapter 3: Using the Legacy MobilePASS Factory

Resetting token serial numbers

Each time an authenticator is generated, MobilePASS assigns it a serial number based on the current license. The license_counter.ini file found in \<install_dir>\data\config directory, contains the next token serial number to generate. The license is a range of serial numbers, and as authenticators are generated, MobilePASS moves sequentially through that range, choosing serial numbers. License_counter.ini tracks where in the range the next generated authenticator serial number will be assigned.

There are a variety of reasons for which you may need to reset the license counter. For example, if all licensed serial numbers have been used and an employee who had been assigned a serial number in that range leaves the company, you could reset the counter to the departing employee’s serial number. To do this, you would go to license_counter.ini, set the next serial number to the desired serial number in the range, and restart the MPF service. The authenticator could then be assigned to someone else.

**Tip:** To reset the counter and force the MobilePASS Factory to generate tokens using the first serial number, delete the data/config/license_counter.ini file, and then restart the MPF. Reset the counter to begin with the first serial number or any number in the series.

Importing token data to SafeWord

MobilePASS can produce two types of token import records (depending on whether they were batch or user-generated) that must be imported into the SafeWord server before users can authenticate. Those files are:

- **mpimport.dat** (if user-generated) found in \<install_dir>\data\output.
- **import.dat** (if batch-generated), found in a sub-directory of \<install_dir>\data\output (with a naming convention that includes type, number of tokens, date (YYYY_MM_DD), and time (in 24-Hr format HH_MM_SS).

**Note:** If the mpimport.dat file is renamed, the name must also be changed in mobilepass.ini.

The basic process for importing token data files using the SafeWord 2008 Management Console is as follows:

1. Launch the console (Start > Programs > Aladdin > SafeWord > SafeWord 2008 Management Console).
2. Select File > Import, then choose Software/Hardware Authenticators.
3. Browse to (locate) the token data file, select an Admin Group into which you want to import the files.

What’s Next?

At this point, MobilePASS is ready to be deployed to end users. You may choose to deploy authenticators in two manners:

• You can generate a batch of authenticators and send them to end users as device-specific packages.

• You can provide end users with the end user authenticator download page URL and users can generate, download, and install their own authenticators.

“Deploying the software” on page 87, provides instructions for both deployment methods.
Understanding MobilePASS packages

You deploy MobilePASS to end users in the form of device-specific packages. The packages contain the necessary files for installing MobilePASS. Installing the software will vary by device type, and end users should consult their device’s operating instructions when they install MobilePASS.

Additionally, MobilePASS Messaging can be used as a method of transmitting passwords to users’ mobile devices.

**Important:** Some of the device package information described in this chapter will need to be distributed to end users.

MobilePASS is available for the following types of devices:

- Windows Desktops
- BlackBerry devices
- J2ME devices
- Smartphones
- Pocket PCs

**Inside the MobilePASS for Windows Desktops package**

MobilePASS for Windows Desktops is designed to run on Windows 2003/2008, Windows XP Professional/Home, and Windows Vista (32-bit and 64-bit) platforms. The package contains two files – `MobilePass.exe` and `mpconfig.ini` – are packed as a zipped file when a MobilePASS for Windows Desktops authenticator is generated.

**Important:** The `mpconfig.ini` file must always be installed in the same directory as the MobilePASS executable.

**Inside the MobilePASS for BlackBerry package**

MobilePASS for BlackBerry is designed for use with RIM BlackBerry devices running OS version 3.8 or higher. The MobilePASS package contains two files: `SccJ2ME.cod` and `SccJ2ME.alx`, both of which are necessary to download and activate MobilePASS on the BlackBerry device.
Inside the MobilePASS for J2ME package

MobilePASS for J2ME is designed for use on mobile devices enabled with Sun’s Java 2 Micro Edition Platform or Micro Edition Support (CLDC 1.1/MIDP 2.0). The MobilePASS for J2ME package is comprised of two files: SccJ2ME.jar and SccJ2ME.jad. Both files are needed to activate MobilePASS. Please refer to the device manufacturer’s instructions for installing applications.

Inside the MobilePASS for Smartphones package

The MobilePASS for Smartphones package is designed for devices running Windows Mobile version 5.0 or later. The package contains two files, MobilePass.exe and mpconfig.ini. These files are packed as a zipped file when a MobilePASS for Smartphones authenticator is generated.

**Important:** The mpconfig.ini file must always be in the same directory as the MobilePASS executable.

Inside the MobilePASS for Pocket PCs package

The MobilePASS for Pocket PCs device package is designed for devices running Windows Mobile version 5.0 or later. The package contains two files, MobilePass.exe and mpconfig.ini. These files are packed as a zipped file when a MobilePASS for Pocket PCs authenticator is generated.

**Important:** The mpconfig.ini file must always be in the same directory as the MobilePASS executable.
Deploying the software

MobilePASS authenticators can be deployed in two methods:

- You can generate a batch of authenticators and send them to end users as device-specific packages.
- You can provide end users with the end user authenticator download page URL, and users can generate and download their own device packages.

If PINs will be required for use with passcodes, you will need to convey that information to the end users. PIN requirements are based on the token parameter configurations set in the `mpdefaultparam.ini`.

**Security Alert:** For security purposes, you should distribute device packages to end users separately from authenticator PIN information.

Both deployment methods result in the generation of MobilePASS device-specific packages that are ready to be installed on end user devices.

Generating batches of authenticators

You can generate batches of authenticators and then e-mail the packages to your users for installation on their devices. The batch method is best suited for situations where a number of users will be authenticating using the same type of device. Before generating authenticators, you should do the following:

- Organize MobilePASS users into groups based on the type of device package.
- Ensure the current MobilePASS license meets or exceeds the number of users for whom authenticators will be generated. (See “Adding an additional license” on page 79 if additional authenticators are needed.)

To generate a batch of authenticators, from **Start > Programs > Aladdin > MobilePASS > MobilePASS Factory**.

![Figure 88: MobilePASS Factory window](image)

Welcome to the MobilePass Factory

From this page, you may accomplish the following:

- Generate authenticators
- View current license or add another license

You may also view end user pages:

- View the end user authenticator download page
- View the Messaging and new authenticator request page
- View the Messaging end user password request page

1. Select **Generate authenticators**.
2 In the Batch Generation window, select a platform from the **Select a platform** menu.

In Figure 89, MobilePass for Smartphones is selected.

3 Enter the total number of authenticators for this batch in the **Number of Authenticators** field.

**Note:** *The current MobilePASS configuration parameters are displayed in the lower portion of the window.*

4 Click the **Start Generation** button.
The MPF processes the request and generates an *import.dat* file. The data is placed in a uniquely-named directory based on the selected platform, the number of authenticators, and the generation date and time.

**Figure 90:** Successful Batch Generation Window

Figure 90 shows a successful batch generation. The first file displayed in the window, the *import.dat* file, contains all token records for the generated batch of authenticators. You must import this file into the SafeWord server. The second file shown contains authenticator serial numbers and the PINs associated with them. This information must be deployed to end users. Both files are stored in the Output folder, which also contains a subdirectory where the MobilePASS packages are stored. You distribute these packages to the end users along with the authenticator information.

**Security Alert:** For security purposes, administrators distributing device packages to end users should deliver the authenticator PIN information separately from the device packages.
Using the end user authenticator download page

The end user download page is designed to allow individual users to generate MobilePASS authenticators and download them for installation on their devices. With this approach, the users themselves are responsible for and allowed to obtain the necessary package(s) for their device.

**Note:** Before allowing end users to generate and download MobilePASS device packages, you must ensure the MobilePASS license has sufficient authenticators available for all the end users.

To view the end user download page:

1. On the MPF Welcome window, click the View the end user authentication download page option.
   The MobilePASS Authenticator Download page displays, and allows users to generate and download their own authenticators.

   ![Figure 91: MobilePASS Authenticator Download page](image)

   **MobilePass Authenticator Download**

   You must choose a platform and supply a user name to generate your new authenticator.

   Select a platform: [MobilePass for Smartphones]

   Enter your user name: [Enter user name]

   Generate Authenticator

2. Copy and save the URL (in the Address field at the top of the window), and send this URL to end users along with instructions to launch this page, select their desired platform, enter their user name, and select the Generate Authenticator button.

   MobilePASS processes the request, and displays the successful activation as shown in Figure 92.
Figure 92: Successful Activation window

If you configured MobilePASS to require that users attach a PIN to passcodes, that PIN also appears on the window.

**Important:** If a user forgets their PIN, you can refer to the `audit.log` file, which is stored in the Output folder. This file contains a list of all the authenticators that were successfully generated from the end user download page. The user name and the authenticator serial number and PIN associated with it are contained in the file.

3. Tell your users to note and memorize their PIN, and then select the link(s) to download MobilePASS for their device.
   
   In Figure 92, selecting **MobilePASS for Smartphones** downloads the software to the end user’s computer.

4. The users should consult their device’s user guide for instructions on how to install MobilePASS.

Installing MobilePASS on end user devices

Once the MobilePASS package contents have been saved to the user’s computer, MobilePASS can be installed on the user’s device. End users should refer to their device user guides for specific installation instructions.
In addition to the general configuration options that are available for the MobilePASS Factory, certain device options can also be customized. The sections that follow describe these options.

**Note:** The MobilePASS Factory service must be restarted after customizing the options for the device-specific packages.

### Customizing MobilePASS for Windows Desktops

The Windows Desktops device package can be customized before deployment. The customizable `mpconfig.ini` file is located in `<install_dir>/data/templates/device/win`.

**Important:** Custom skin and button files can be renamed, but in the `mpconfig.ini` file, everything must be case sensitive and labels should not be modified.

### Customizing the token appearance

The token appearance can be customized in the `mpconfig.ini` file using Microsoft Notepad or another text editor. Specific details about the parameters are included in the configuration file.

### Customizing additional options

MobilePASS for Windows Desktops options can be customized in the `mpconfig.ini` file. As with all the parameters, the configuration file provides the parameter options, parameter descriptions, and parameter details. Microsoft Notepad or another text editor can be used to make changes to the file. The following parameters can be customized:

- Passcode clipboard copy: automatically copies passcodes to the clipboard
- Run in system tray: runs MobilePASS in the system tray on the desktop

When you are finished customizing the token options, the MPF service must be restarted.
Customizing MobilePASS for J2ME devices

The MobilePASS for J2ME device package has two options that may require customization. One sets the size of the MobilePASS icon that displays on some J2ME-enabled devices, the other sets the font size of displayed passcodes.
Changing the MobilePASS icon size

On some J2ME-enabled devices, the MobilePASS icon may either not appear or may appear larger than desired. To change the icon for best display size, do the following:

1. Browse to the SccJ2MExxxxx.jad file that was downloaded with the MobilePASS for J2ME package.
2. Open the file with Microsoft Notepad or another text editor.
3. Locate the MIDlet-1 property.
4. Select the SIcon.png value in the MIDlet-1 property line.
5. Change the selected value to SIconSmall.png.
6. Locate the MIDlet-Icon property.
7. Select the SIcon.png value in the MIDlet-Icon property line.
8. Change the selected value to SIconSmall.png.
9. Save the file and reinstall the J2ME package on the device.

Changing the passcode font size

On some J2ME-enabled devices, the font size of displayed passcodes may need to be customized. To change the font size:

1. Browse to the SccJ2MExxxxx.jad file that was downloaded with the MobilePASS for J2ME package.
2. Open the file with Microsoft Notepad or another text editor.
3. Locate the mpFonts property.
4. Select the default value in the mpFonts property line.
5. Replace the selected text with one of the following values:
   - large
   - small
   - medium
6. Save the file and reinstall the J2ME package on the device.
Symbols
.jad file 31

A
activating MobilePASS for Pocket PCs 86
activating MobilePASS on J2ME devices 86
activating MobilePASS on the BlackBerry device 85
activation code 24
activing MobilePASS for Smartphones 86
allowing self-enrollment 10
Android 4
Android MobilePASS
activating 59
changing PIN 63
generating passcodes 61
installing 57
resetting 65
Apple Store 23
audit.log file 91
authenticators
evaluation 75
auto-enroll 35
automatic authentication 40

B
BES 40
auto-enrollment parameters 35
enabling automatic authentication 40
BES policy 31
editing 34, 37
BlackBerry devices 4
BlackBerry MobilePASS 31
activating 41
change PIN 45
changing PIN 45
deploying 31
downloading and installing 40
generating passcodes 44
resetting the token 46

C
Changing PINs 29
CLDC 1.1/MIDP 2.0 47
customizing
token interface window 92

D
deploying MobilePASS 85

E
Enrollment Portal 10, 16
Enterprise Solution Pack 74
evaluation token file
SafeWord 2008 5
SafeWord PremierAccess 5
evaluation tokens
SafeWord 2008 software and messaging tokens 5
SafeWord PremierAccess software tokens 5

G
generating batches of authenticators 87
generating individual MobilePass authenticators 90
I
importing records to SafeWord 83
install MobilePASS 23
installing MobilePASS 91
iPhone MobilePASS
activating 24
change PIN 29
generating passcodes 28
installing 23
resetting 28
iPhone/iPod touch devices 4

J
J2ME devices 4
J2ME MobilePASS 47
activating 48
Change PIN 52
changing PINs 52
deploying 47
generating passcodes 51
installing 47
resetting the token 53

M
Mac OS 4
Messaging 70
Messaging token 4
messaging.ini 71, 81
MobilePASS
adding additional licenses 79
and PINs 87
compatibility 74
component specifications 74
deploying 87
downloading 76
end user authenticator download page 90
end user download page URL 90
import.dat file 89
installing 76
installing on end user devices 91
installing on iPhone/iPod touch devices 23
license_counter.ini 83
licenses 87
packages for end users 89
PIN behavior, changing 82
PINs 89, 91
requirements 74, 76
MobilePASS Factory 4, 81
MobilePASS Factory service 82
MobilePASS for BlackBerry 85
MobilePASS for J2ME 86
MobilePASS for Pocket PCs 86
MobilePASS for Smartphones 86
MobilePASS for Windows Desktops 85
MobilePASS Messaging 81
MobilePASS Portal 10
MobilePASS Route 70
mobilepass.ini 81
MobilePASS
end users
downloading authenticators 90
mpconfig.ini 92
mpdefaultparam.ini 81

O
Over the Air (OTA) deployment 31

R
reenroll software tokens
configuring to allow 21
resetting
iPhone MobilePASS token 28
resetting license_counter.ini 83

S
serial numbers 89
SMS 70, 81
SMTP 70, 81
Software token 4

test software token 19
token
interface windows 92
token serial numbers 83
V
Vista 4

W
webconfig.ini 82
Windows Phone 4
Windows XP 4