Contacting SafeNet

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance you can contact the SafeNet technical support team help-desk which is available 24 hours a day, seven days a week:

<table>
<thead>
<tr>
<th>Country/Region</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>+1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>+1-410-931-7520</td>
</tr>
</tbody>
</table>

For further assistance submit additional questions to the SafeNet technical support team at the following web page:

http://c3.safenet-inc.com/secure.asp

For assistance via email to SafeNet technical support send the request to the following address:

support@safenet-inc.com
# Table of Contents

**Introduction** ................................................................................................................................................. 7

Overview .......................................................................................................................................................... 8
PGP Desktop and eToken ................................................................................................................................... 8
Integration Requirements and System Prerequisites ...................................................................................... 8

**Setting Up PGP Desktop for Use with eToken** ............................................................................................ 9

Installing PGP Desktop .................................................................................................................................... 10
Generating PGP Keys ..................................................................................................................................... 12
Adding a New User and Encrypting the Disk .................................................................................................. 16
Testing the Setup ............................................................................................................................................. 19
This guide describes the integration and use of PGP Desktop 10.1 with eToken and SAC 8.0 SP1 in hard-disk encrypted mode using preboot authentication.

In this chapter:

- Overview
- PGP Desktop and eToken
- Integration Requirements and System Prerequisites
Overview

Mobile computers are quickly emerging as the industry standard for increasing user productivity. However, the portable nature of these devices increases the possibility of loss or theft. Consequent exposure of sensitive data can result in financial loss, legal ramifications, and brand damage.

PGP Whole Disk Encryption provides enterprises with comprehensive, nonstop disk encryption for Microsoft and Apple Mac OS X, enabling quick, cost-effective protection for data on desktops, laptops, and removable media. The encrypted data is continuously safeguarded from unauthorized access, providing strong security for intellectual property, customer and partner data, and corporate brand equity.

PGP Desktop Professional is a comprehensive suite of encryption applications to protect sensitive data in email, instant messages, and on disk or removable media. PGP Desktop Professional secures confidential information wherever it exists, protecting sensitive information and helping to meet partner and regulatory mandates for information security and privacy.

PGP Desktop and eToken

Organizations using PGP Desktop Professional are now able to store their PGP keys securely on a Safenet eToken, the only authentication device of its type offered to PGP customers using PGP Whole Disk Encryption. Users simply store their PGP keys on the eToken and plug in the token, requiring users to remember only one password - the eToken password.

This partnership between PGP Corporation and Safenet enables customers from around the world to purchase both their PGP Desktop Professional software and eToken devices directly from PGP authorized partners, providing powerful security, an unparalleled level of convenience, flexibility, and productivity, as well as huge cost-savings.

Just as executives carry the keys to their car, they are now able to gain peace of mind by literally carrying the key to their laptop. Using eToken with PGP adds the much-needed layer of additional physical security - both generating and storing PGP encryption keys on the token itself. Users can easily and securely carry numerous PGP credentials to multiple machines, also using eToken for any number of security applications, including network logon, VPN/Web access, password management, PKI solutions, and more.

Integration Requirements and System Prerequisites

This integration was performed using PGP Desktop 10.1, Build 860.

For the instructions provided in this guide to succeed, the following programs must be pre-installed and configured on the client computer:

- Windows XP SP2
- SAC 8.0 SP1
Chapter 2
Setting Up PGP Desktop for Use with eToken

This chapter describes how to install PGP Desktop on the client computer, generate the PGP keys on the eToken, encrypt the local hard disk, and perform preboot authentication to test the setup.

In this chapter:

- Installing PGP Desktop
- Generating PGP Keys
- Adding a New User and Encrypting the Disk
- Testing the Setup
Installing PGP Desktop

The first step is to install PGP Desktop 10.1, Build 860.

To install PGP Desktop:

1. Run the PGPDesktopWin32-10.1.0.exe file.

   The *PGP Desktop* window opens.

2. Select the preferred language.

   The *License Agreement* window opens.

3. Accept the license agreement and click *Next*.
The Display Release Notes window opens.

4. Click Next.

The Updating System window opens.

5. When the system update is complete, the Installer Information window opens.

6. Click Yes to restart the computer.
Generating PGP Keys

This stage includes generating a public key and an associated private key on the eToken. If required, the public key can be published in the PGP Global Directory.

To configure PGP Desktop:

1. In the Windows Start menu, select Programs > PGP > PGP Desktop.
   The PGP Desktop window opens.

2. In the left pane, select PGP Keys > All Keys.
   The PGP Desktop - All Keys window opens.

3. In the File menu, select New PGP Key.
   The PGP Key Generation Assistant window opens.

4. Insert the eToken.
When the eToken is detected, the **Generate Key on Token** indicator is selected, displaying **Safenet Inc. eToken**.

5. Click **Next**.

The **Name and Email Assignment** window opens.

![Name and Email Assignment window](image)

6. Specify the full name and email address to be associated with the key pair, and click **Next**.

The **Create Passphrase** window opens.

![Create Passphrase window](image)

7. Type the eToken PIN as the passphrase, and click **Next**.
The Key Generation Progress window opens and the keys are generated.

The key generation process completes.

8. Click Next.
The PGP Global Directory Assistant window opens.

9. Click Next to publish your public key to the PGP Global Directory.

**Note:** If you do not want to publish your public key at this stage, click Skip.

The PGP Server Progress window shows the progress of the publishing process.

When the key is successfully published, the Progress window opens.

10. Click Next.

The PGP key generation process is complete.
Adding a New User and Encrypting the Disk

The eToken user is now defined as a new PGP Desktop user, and the hard disk is encrypted.

To add a new PGP Desktop user and encrypt the disk:

1. In the left pane of the PGP Desktop window, select PGP Disk.

**Note:** Ensure that the eToken is still connected.

The Encrypt Whole Disk window opens.

2. In the right pane, click Add User Key.

The Add Key Users window opens displaying the newly-created user in the left pane.
3. Select the user that you want to add and click **Add**.

   The user is added to the list on the right.

![Add Key Users](image1)

4. Click **OK**.

   The user is added to the *User Access* list in the lower section of the *Encrypt Whole Disk* window.

![Encrypt Whole Disk](image2)

5. Click **Encrypt** in the top right section of the window.

   The *PGP Whole Disk Encryption* window displays information on the disk encryption process.
6. Click **Yes**.

The *PGP Enter Passphrase for Key* window opens.

7. Type the passphrase for the key (the eToken PIN), and click **OK**.

The disk encryption process starts.
When the encryption process is complete, the *Encryption Progress* sub-window closes.

---

**Testing the Setup**

You can now test the preboot authentication setup.

**To test the preboot authentication:**

1. Restart the computer.

   The PGP preboot authentication window opens.

   ![Preboot Authentication Window](image)

2. Make sure the eToken is attached.

3. Type your passphrase (the eToken PIN), and press **CTRL+Enter**.
Windows XP starts to boot after successful authentication in the PGP Pre-boot stage.