

## Full disk encryption with Sophos Safeguard ® Enterprise With Two-Factor authentication of Users Using SecurAccess by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview	
	Arlington Business Park	
	Theale	
	Reading	
	RG7 4TY	
Phil Underwood	Punderwood@securenvoy.com	



# Contents

Content Sophos	s SafeGuard ® Enterprise Integration Guide	23
Pre Req	UISITES	4
Sophos 1.1 1.2 1.3 1.4 1.5	SafeGuard Enterprise Installation of Sophos SafeGuard Enterprise v6.0 Sophos SafeGuard Management Centre Create A Sophos Client Package Installation of Sophos SafeGuard client software Sophos SafeGuard User Interface and client operation	4 4 5 5 5
1.5.1	User logon with Sophos Pre Boot Authentication	6
SecurEr 2.0 2.1 2.2 2.3 2.3	Novy Security Server Configuration of SecurEnvoy Pre requisites for SecurEnvoy Server SecurEnvoy Server Configuration Test SecurEnvoy Can Logon To Sophos Safeguard SecurEnvoy User configuration	6 6 6 7 7
3.0 3.1 3.2	End User experience User experience - Daycode updated User Logon scenarios	8 9 9
4.0	Disable Windows Change Password 1	.0



## **Sophos SafeGuard ® Enterprise Integration Guide**

This document describes how to provide additional security to Full disk encryption by Sophos SafeGuard ® Enterprise by fully integrating SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Sophos SafeGuard ® Enterprise provides protection to corporate data by enabling Full disk encryption and pre boot authentication of P.C.'s and laptops.

SecurAccess provides two-factor, strong authentication for Sophos SafeGuard ® Enterprise, without the complication of deploying hardware tokens or smartcards. Two-Factor authentication is provided by the use of your PIN and your Phone to receive the one time passcode.

SecurEnvoy Security Server is configured to use "Direct Password Control" such that it can take control of both the Microsoft password and Safeguard password. By applying an alphanumeric User PIN of between 4 to 8 characters and a 6-digit (or character) passcode together, this is then saved as the new Microsoft and Safeguard password. The passcode is then updated on a per day or multiple days frequency, each time this is added to the existing user Pin and then written as the Microsoft and Safeguard password. Therefore the Safeguard POI password is now using Two-Factors and is changing on a daily or multiple day basis.

"Direct Password Control" will change and send out the new Domain password via SMS or email to all enabled users. This is the dynamic component of the Domain login; a separate static Pin is required to make up and complete the Domain authentication, which is managed by SecurEnvoy. Setting the correct level of upper and lower case characters as well as numeric allows the passcode to meet Domain Security policy requirements.

The security strength of the password controlled by SecurEnvoy can be configured to be as low as 10 characters, the first 4 being an alphanumeric pin followed by a 6 digits code or as high as 14 characters, 8 being the pin followed by an alphanumeric passcode. These passwords are significantly stronger that a standard user created password as they are based on two factor authentication with no single part being stored or written down in any one place and the passcode part does not use easy to crack dictionary words.

Offline laptops that are out of contact with Safeguard are managed by SecurEnvoy by tracking and displaying both the laptops off-line passcode and the current online passcode. Note that only one laptop per userid is supported.

#### The equipment used for the integration process is listed below:

**Microsoft** (for installation of SecurEnvoy Security Server and Sophos SafeGuard) Windows 2008 server IIS installed with SSL certificate (required for management and remote administration) Access to Active Directory with an Administrator Account Windows 7 Enterprise 64 bit (Installation of Sophos client)

#### Sophos SafeGuard ® Enterprise

Sophos SafeGuard Enterprise Server v6.0 Sophos SafeGuard Client v6.0

#### SecurEnvoy

SecurAccess software release v6.2.502



# **Pre Requisites**

It is assumed that the Sophos SafeGuard <sup>®</sup> Enterprise v6.0 is setup and operational. It is also assumed that SecurEnvoy server version 6.2.502 or higher has been installed on the same server with a suitable account created that has read and write privileges to Active Directory.

NOTE: SecurEnvoy only supports Two-Factor authentication with Sophos SafeGuard Enterprise using DAYCODE passcodes sent via SMS or eMail. Daycodes are the only supported method; one time codes (OTP) and soft tokens are not supported.

NOTE: Only One SafeGuard Encrypted Device is supported per UserID.

## **Sophos SafeGuard Enterprise**

### **1.1** Installation of Sophos SafeGuard Enterprise v6.0

Launch the Sophos SGNInstallAdvisor, this will show the following screen.

Sophos - SafeGuard Enterprise	Installation Advisor 6.00.0			_02
SOPH WWW.SOPHC	OS ps.com	ß	English - German	2
Welcome to the SafeG	uard Enterprise Installation Ad	lvisor		
General Information	This tool is designed to help op it provides a Step-by-Step insta Existing environments have to be up Hints: -Please start the Installation Advisor -Follow the installation order to avoi -Supported operating systems: Win 2003 R2 Server (28 and 64 bit d6tb Windows Server 2008 Server 30 R4 2 (64 bit).	vu Install a SafeCoard Enterprise environment. Illiation for a new installation. pdated as described in the installation manual. In with Administrative Rights. Id additional configuration alsos. dives 2003 Server (20 and 64 bit editions). Windows ons). Windows Server 2008 (32 and 64 bit editions) a	Find a Partner     Download Documentation     Open Release Notes nd	
Prepare the Server				
Set up SafeGuard Ent	erprise			
Install a Client				
	Copyright 1996-2012 Sophos Group. All rights	s reserved. SafeGuard is a registered trademark of S	ophos Group	

Follow the on screen instructions to prepare and install the Sophos software.

For further advice and configuration please use documentation provided by Sophos.

#### 1.2 Sophos SafeGuard Management Centre

Launch the Sophos SafeGuard Management Centre, on first run will prompt for a Security Officer account to be configured and Certificates to be generated.

NOTE: The current Windows logged in account that was used to create the Sophos Security officer is used by later in the guide. It is critical that the correct Windows account is configured for SecurEnvoy services.



Once the Management Centre is operational, this example shows LDAP domain information synchronised to provide a seamless management of Active Directory users and computers.



### **1.3 Create A Sophos Client Package**

Create a Client configuration package.

- 1. Open the Management Centre browse to Tools
- 2. Choose Configuration Package Tool
- 3. Choose create Enterprise Client Package
- 4. Click Add Client Package
- 5. Enter a name for the package
- 6. Select a primary server
- 7. Define the MSI output path
- 8. Click Create Client MSI

For further advice and configuration please use documentation provided by Sophos.

### 1.4 Installation of Sophos SafeGuard client software

The client installation requires the following:

Sophos SafeGuard Preinstall package Sophos SafeGuard Client package Sophos SafeGuard Client Configuration package (Generated by primary Sophos SafeGuard server)

Organize 🔻		:= 🗸 🔞
Name	Publisher	Installed On
💿 Sophos SafeGuard 6.00.0 Client	Sophos Ltd.	14/06/2012
Sophos SafeGuard 6.00.0 Client Configuration	Sophos Ltd.	14/06/2012
O Sophos SafeGuard 6.00.0 Preinstall	Sophos Ltd.	14/06/2012

## 1.5 Sophos SafeGuard User Interface and client operation

After a reboot, the user will see the following screen:



After the first reboot post Sophos client installation, the user will log in directly to Windows.

Press CTRL + ALT + DELETE to log on 2

Once the Sophos client has synched to the Sophos SafeGuard server a pre boot screen will then be displayed after each subsequent reboot.

Sophos SafeGuard® 6.00 × × Synchronization with Sophos SafeGuard® server succeeded. No new settings available.



### 1.5.1 User logon with Sophos Pre Boot Authentication

After each subsequent reboot the user will be prompted to enter their respective Windows UserID and password into the Sophos logon window.

Once authenticated the user is signed through to Windows once the CTRL-ALT-Del sequence is invoked.

SafeGuar	d Logon - WIN	DOWS7-SE1.LAB.COM
		SOPHOS
<u>U</u> ser name: <u>P</u> assword: <u>D</u> omain:	LAB	
EN Ver. 6.00.0.1	55 <u>R</u> ecovery	20/06/2012 16:27:56 Shutdown Op <u>t</u> ions >>

## SecurEnvoy Security Server

### 2.0 Configuration of SecurEnvoy

#### 2.1 Pre requisites for SecurEnvoy Server

SecurEnvoy Server version 6.2.502 or higher MUST be installed on the same host as Sophos SafeGuard Management Centre as SecurEnvoy integrate via Sophos SafeGuard scripting API.

Microsoft requires that connections to Active Directory via LDAP use SSL (SDLAP 636) to meet password security restrictions. Make sure that "Use SSL" is selected in the LDAP settings "Directory Server Details" in SecurEnvoy Advanced Config

### 2.2 SecurEnvoy Server Configuration

SecurEnvoy require the following to be set up prior to being operational:

- 1. Launch the SecurEnvoy Local Admin GUI, navigate to the Config tab
- 2. Navigate to Soft Token, then deselect "enable soft tokens"
- 3. Navigate to GUI settings, then select "Display Offline laptop"
- 4. Navigate to PIN management, then select SecurEnvoy as the PIN, finally set the PIN length to at least 4 digits and set these to be at least 1 upper and 1 lowercase.
- 5. Navigate to Daycode, un-tick "Only send a new code if last used" set the default user days, validity of Daycode (1-99 days)
- 6. Navigate to Tmp Static Code and select "Return To Day Code"
- Navigate to Direct Password Control, enable PIN and Passcode synched to user password, enable sync to Sophos. Set Sophos Security Officer details, as tested in 1.2
- 8. The Windows account (Logged on user) that was used when the Sophos Security Officer was generated is required as the "Log on" account for the following Window services:
  - a. SecurEnvoy Batch server service
  - b. SecurEnvoy Web SMS and or Phonegateway service



Start - Administration Tools - Services, select each service shown above and right mouse click, go to properties, select log on and enter details of the Windows account.

- 9. The file permissions of SecurEnvoy/Security Server and all sub directors must have full r/w access for the windows account set in step 8
- 10. If you require alphanumeric passcodes then edit server.ini and set UseAlphanumericPasscodes=True

#### NOTE: These services will have to be restarted to use the new "log on" settings

NOTE: The windows account used for these services must not change its password or these services will fail. Make sure this windows account has "Password never expires" selected in Active Directory Users and Computers

### 2.3 Test SecurEnvoy Can Logon To Sophos Safeguard

Check the Sophos Security officer account created in step 6 can be authenticated via the SecurEnvoy test tool. Navigate to the SecurEnvoy\Security Server\Sophos directory and run the testlogin.exe program.

If operation is correct an "OK" will be displayed.

### 2.3 SecurEnvoy User configuration

Launch SecurEnvoy local admin GUI, search for desired user that requires Two-Factor authentication with Sophos SafeGuard. The following screen will be displayed. Enable the user, enable Off-line Laptop check box. Create a PIN

# NOTE: To meet a domain password policy, it is recommended that the PIN is a combination of both upper and lower case. Example PIN = Se12, Passcode = 234765, Domain password = Se12234765

Set the user's mobile number if	Manage User Phi	IU@lab.com	User has never authenticated
not already populated in Active	(CN=PhilU CN=Users DC=lab	DC=com)	
	O Unmanaged	O Disabled O Enabled	In Case of Emergency
Set the user to use a Daycode	Administrator HelpDesk Group	None HelpDesk Config	Change Group
and set time period (1-99 days)	Off-Line Laptop Pin 4 Digit	Create Pin	User Create Pin
	Send Code To Mobile Send Code To E-Mail	• +447917035921	Private Number 🗹
Click update when complete	Send Simple SMS Text Failed Login	<ul> <li>(Some countries can't deliver dyna</li> <li>(Reset To Zero </li> </ul>	amic sms text)
The following message will be displayed:	One Time Code Soft Toker	e ● Best Security Use Real Time ● ● SecurEnvoy Only ReSyn	e Not Preload 🗖
"Passcode sent to Gateway, Windows password updated"	Day Code Tmp Static Code Static Code	Code every 1 days Inclué     Passcode     Passcode     (m	de Sat & Sun 🗖 ays nax 14)
	Update	Resend Passcode	Refresh



### 3.0 End User experience

Once the user has been set up and deployed upon the SecurEnvoy server, they will receive a SMS message as shown below:

🗤 vodafone UK 🛜 12:40				
Messages 447764390996 Edit				
Call Add to Contacts				
Text Message 21 Jun 2012 12:24				
Active Passcode 075964 Backup Passcode UNKNOWN				

The SMS will display the Active passcode and a Backup passcode.

**NOTE:** The Backup passcode will be blank until the SecurEnvoy Batch server has run and trapped the previous Daycode, this is required for accessing a laptop when the Windows Password (SecurEnvoy) has been updated but the laptop was offline.

After a reboot the user will be prompted for a Windows user logon

User enters their UserID into the UserID field and PIN followed by the passcode into the password field, the passcode is displayed in the SMS message.

Example Se12075964 Where Se12 is the PIN and 075964 is the passcode



The Sophos SafeGuard client runs in the Windows "Systray" after a reboot it will show the following message. This shows that the client has now synched to the Sophos SafeGuard server.

Throughout the day the user may see the following message. This shows that s synchronisation has been successful, but no new settings were obtained. Sophos SafeGuard® 6.00 \* × Synchronization with Sophos SafeGuard® server succeeded. New certificate received.

Sophos SafeGuard® 6.00 \* × Synchronization with Sophos SafeGuard® server succeeded. No new settings available.



After a reboot, the user will be prompted for Pre Boot Authentication.

SafeGuard Logon - WINDOWS7-SE1,LAB.COM	User enters their UserID and PIN followed by the Active passcode displayed in the SMS
$\bigcirc J$	message.
SOPHOS	Example Se12075964 Where Se12 is the PIN and 075964 is the passcode
User name:	
Password: LAB	
EN         Ver. 6.00.0.155         20/06/2012 16:27:56           OK         Recovery         Shutdown         Options >>	

Once authenticated the user is signed through to Windows once the CTRL-ALT-Del sequence is invoked.

### 3.1 User experience - Daycode updated

When the SecurEnvoy server updates the Daycode (default 16:00 local time) the configured user(s) will receive a new SMS message as shown below:

📲 vodafone UK 🗢 13:11 📼			
Messages 447764390996 Edit			
Call Add to Contacts			
Text Message			
Active Passcode 364257 Backup Passcode 321620			

The SMS will display the Active passcode and a Backup passcode.

The user should always try and use the new passcode unless they receive a logon error, at which point they should then use the Backup passcode.

#### 3.2 User Logon scenarios

Listed below are some of the scenarios a user may see during the operation of the SecurEnvoy server and the Sophos SafeGuard Server. All logons require PIN + PASSCODE

a)	User is logged on when Daycode is
	updated. They will see the following
	message.
	When the log's off and log on again they
	will then use the new Active Passcode

Sophos SafeGuard® 6.00 \* × Synchronization with Sophos SafeGuard® server succeeded. New certificate received.



 b) User had machine 'Locked' when Daycode was updated, user logs in with new Active Daycode is SMS message.
 Sophos will then prompt the user to

enter the Backup Daycode to ensure synchronisation and correct operation.



c) User has their machine switched off when the Daycode is updated, user logs in with new Active Daycode is SMS message.

> User then receives an "Authentication error" user then logs in with the Backup Daycode.

SafeGuard Logon - WINDOWS7-SE1,LAB.COM		
0)		SOPHOS
		2011102
<u>U</u> ser name:		
<u>P</u> assword:		
<u>D</u> omain:	LAB	•
EN Ver. 6.00.0.	155	20/06/2012 16:27:56
	Recovery	<u>S</u> hutdown Op <u>t</u> ions >>

Once authenticated the user is signed through to Windows once the CTRL-ALT-Del sequence is invoked.

If the machine is online and able to contact a Windows Domain controller the user will get a Windows logon error as the password (Daycode) is now out of sync.

The user now logs in with the Active Daycode.

Once authenticated the user will see the following message from the Sophos SafeGuard client in the "Systray". Synchronisation is complete and the Daycodes (passwords) are now in step with each other.



Sophos SafeGuard® 6.00 \* × Synchronization with Sophos SafeGuard® server succeeded. New certificate received.

### 4.0 Disable Windows Change Password

It is recommended that end users do not try and change their Windows password as this process is managed for them. To disable windows change password in the group policy see <a href="http://support.microsoft.com/kb/324744">http://support.microsoft.com/kb/324744</a>