



Symantec PGP Whole Disk Encryption Hands-On Lab V 3.7

Description

This hands-on lab session covers the hard drive encryption technologies from PGP. Students will administer a typical Whole Disk Encryption virtual environment using Symantec Encryption Server and Symantec Encryption Desktop. Use cases and best practices from real world deployments will also be discussed.

At the end of this lab, you should be able to

- Understand the hard drive encryption solution within the Symantec PGP line of products and explain the components of typical deployment using Symantec Encryption Server, Symantec Encryption Desktop, and Whole Disk Encryption
 - Configure and explain the concepts of Users and Groups/Consumer Policy within Symantec Encryption Server
 - Configure and deploy Symantec PGP WDE options and policies
 - Understand Recovery options within the Symantec PGP WDE solution
-
-

Notes

- A brief presentation will introduce this lab session and discuss key concepts.
 - The lab will be directed and provide you with step-by-step walkthroughs of key features.
 - Feel free to follow the lab using the instructions on the following pages. You can optionally perform this lab at your own pace.
 - Do not power off the virtual machines as they will revert to the last snapshot and all progress will be lost. Make sure you only use the reboot functionality, but do not power them off or use the “Shutdown” command
 - Be sure to ask your instructor any questions you may have.
 - Thank you for coming to our lab session.
-

Lab Agenda

The three exercises in this session will take roughly 50 minutes and will include some slide-based instruction.

Exercise 1: Installation / Enrollment

- This lab allows the student to install the Symantec Encryption Desktop software on a virtual machine followed by enrolment.
- Estimated duration: 10 - 15 minutes

Exercise 2: Day to Day Use

- This lab demonstrates how PGP Whole Disk Encryption is used day to day for a normal user and how to adjust/reconfigure policy options centrally and update them on the client.
- Estimated duration: 15 - 20 minutes

Exercise 3: Recoverability Options

- This lab demonstrates the various ways to recover from a forgotten passphrase or bootguard prompt without a user present.
- Estimated duration: 15 - 20 minutes

Lab Exercise 1 - Installation / Enrollment

Estimated duration: 10 - 15 minutes

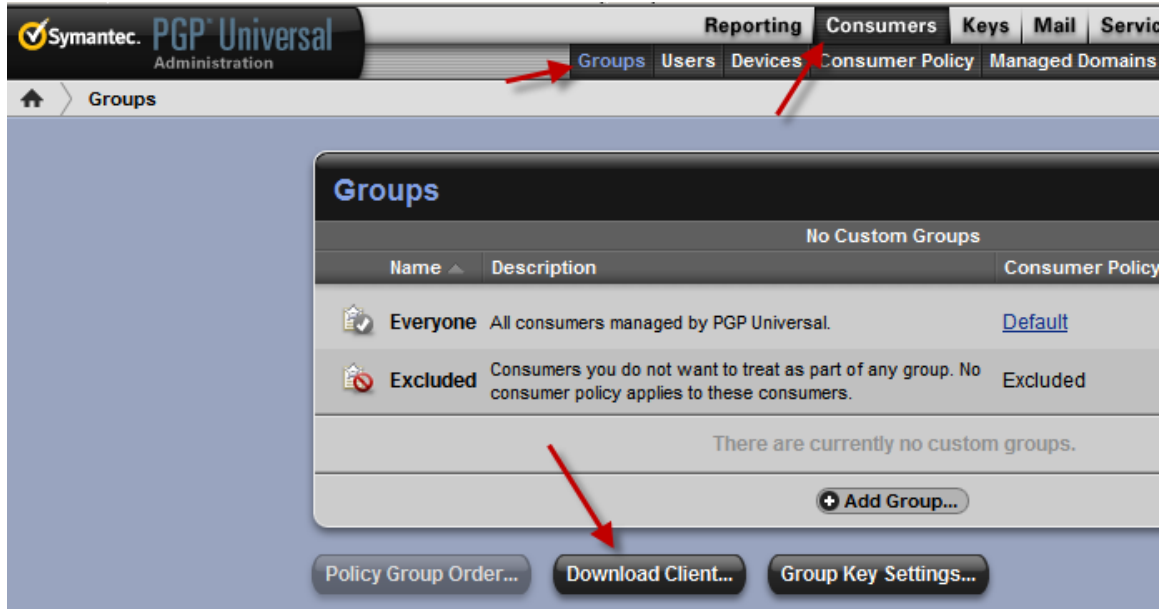
Starting the lab machines

1. If not already running, power on the ***client1*** virtual machine, this is the client computer that will be encrypted. It should be started at the snapshot called "Stage1"
2. If not already running, power on the ***mail.senderdomain.com*** virtual machine, this is the domain controller. It should be started at the snapshot called "Stage1"
3. If not already running, power on the ***keys.senderdomain.com*** virtual machine, this is the Symantec Encryption Management Server, formerly known as PGP Universal Server. It should be started at the snapshot called "Stage1"

Installation

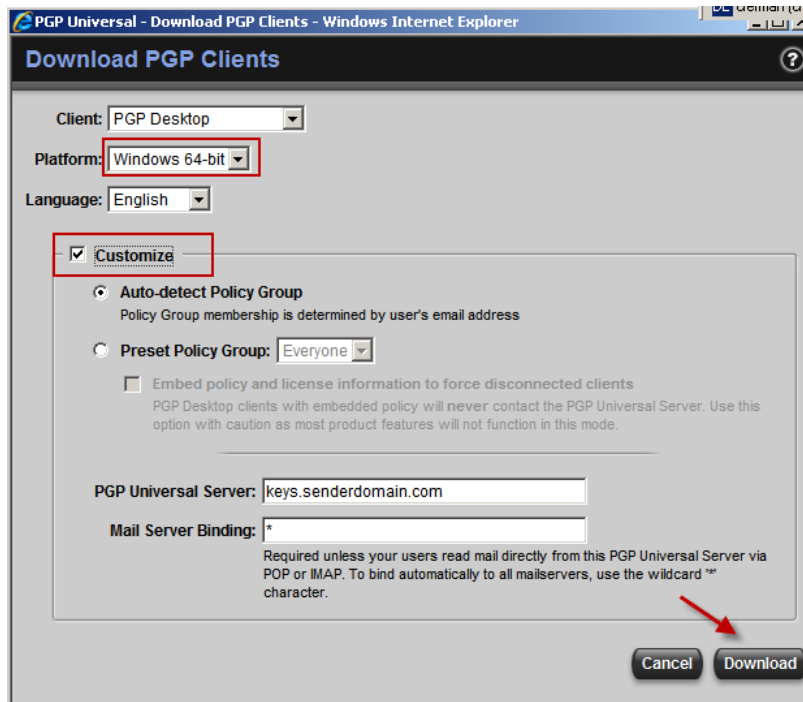
4. Log into the client computer ***client1*** as:
 - a. username: administrator@senderdomain.com
 - b. password: Symc4now!
5. If prompted to reboot at logon, choose to restart later
6. Open the web browser and navigate to <https://keys.senderdomain.com:9000>
7. This will open the Symantec Encryption Server Management Console
8. Login to the Management Console as
 - a. Username: admin
 - b. Password: Symc4now!
9. Go to Consumers - Groups

10. Click **Download Client**



11. Set Client properties:

- a. Windows 64 bit
- b. Select "Customize"
- c. Leave suggested settings for **Auto-Detect Policy Group**, **Symantec Encryption Server** and **Mail Server Binding**



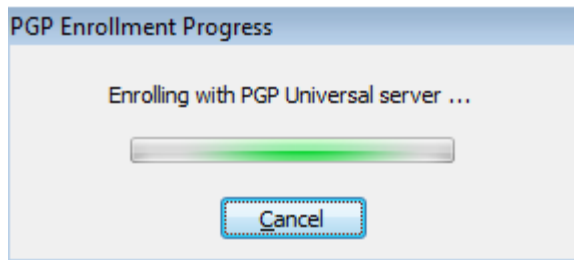
12. Download and save the MSI file to the desktop, do NOT select "Run" in the download dialog box, as the security permissions do not allow an MSI installer to be run directly from the browser session. Download the file to the Desktop.
13. Double click the MSI file to start installation
14. Step through the installation assistant.
15. If requested, confirm to reboot the computer, Symantec Encryption Desktop is now installed.

Enrolment

1. Click "Switch user" and log in to the client computer **client1** as
 - a. Username: "alice@senderdomain.com"
 - b. Password: Symantec1
2. PGP will start as part of the All Users / Startup Folder. As a result of this the PGP Enrollment wizard will appear.
3. In the PGP Enrollment wizard dialog box, enter in the user's AD Password (Symantec1) and press the OK button.

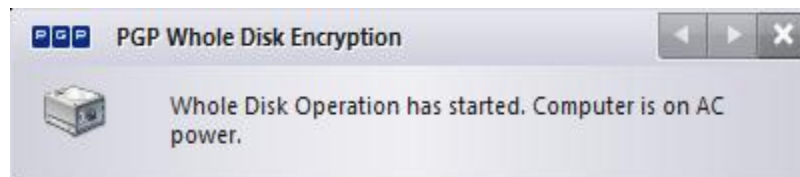


4. The enrollment process will begin and complete with the Symantec Encryption Desktop Notifier box appearing in the bottom right stating Whole Disk Encryption has begun.



To the left is the Symantec Encryption Desktop Enrollment Progress bar. This is the only interaction the user will see once authentication has occurred.

To the right is the Symantec Encryption Desktop Notifier Window. It will display status of the encryption process including starting, pausing, resuming and the completion of the process.



5. Please note that it is possible to configure Symantec Encryption Desktop to perform a fully silent enrollment as well. In this case the user does not have to enter the username or password and no enrollment screens show up. The disk will be automatically encrypted to the user's Windows password and all the user sees is the Symantec Encryption Desktop Notifier as above. For more information consult the following Symantec Knowledgebase Articles:
"HOWTO: Configure PGP Invisible Silent Enrollment"
<http://www.symantec.com/docs/HOWTO77014>
"HOW TO: Enable Silent Enrollment for PGP Desktop Clients"
<http://www.symantec.com/docs/TECH183325>
6. This completes the Installation / Enrolment Exercise. The machine is now encrypting and the user is enrolled successfully. As of now, the boot process is already protected by pre-boot authentication.

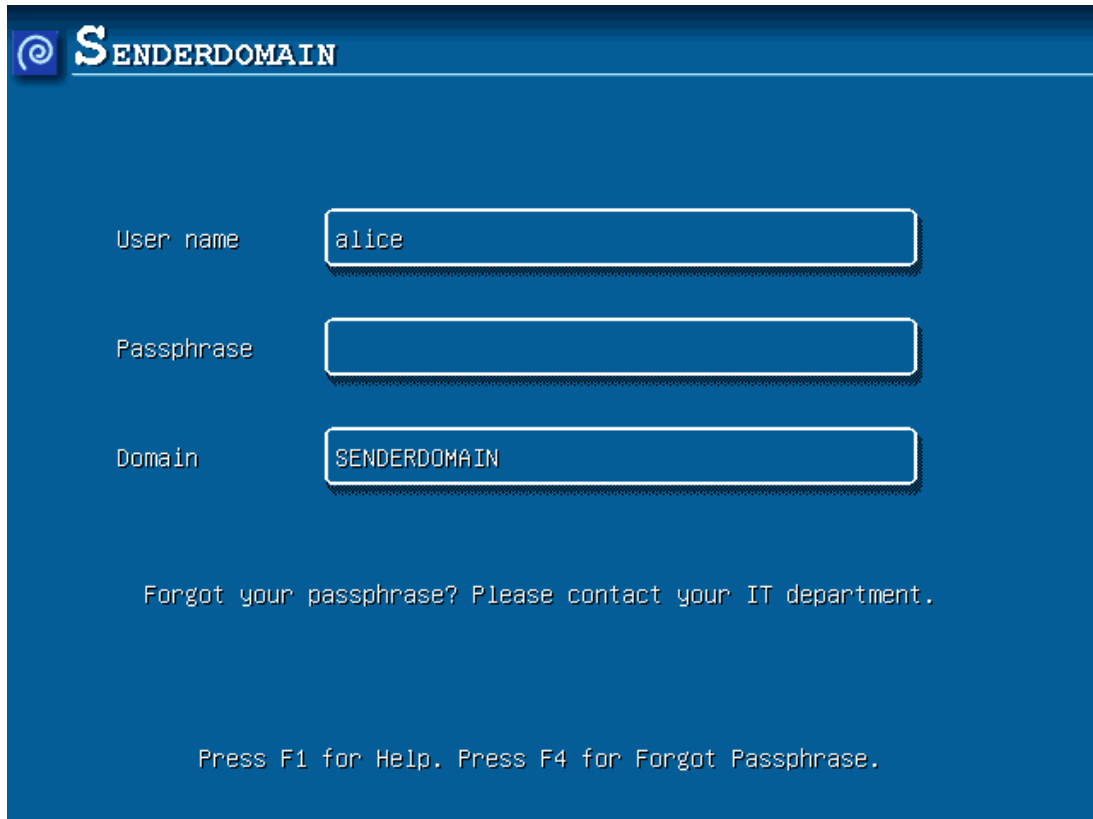
Lab Exercise 2 - Day to Day Use

Estimated duration: 15 - 20 minutes

Pre-Boot Authentication

1. With successful completion of Exercise 1, reboot the **client1** system.
2. After POST, the user will be greeted with a PGP BootGuard screen (in this case the domain-enabled pre-boot screen).
3. (optional) Navigate around the pre boot screen using the F1 and the F4 keys

4. Enter the username, password and select the domain of the user that was enrolled and press enter.
 - a. Username: alice
 - b. Password: Symantec1
 - c. Domain: Senderdomain



SENDERDOMAIN

User name

Passphrase

Domain

[Forgot your passphrase? Please contact your IT department.](#)

Press F1 for Help. Press F4 for Forgot Passphrase.

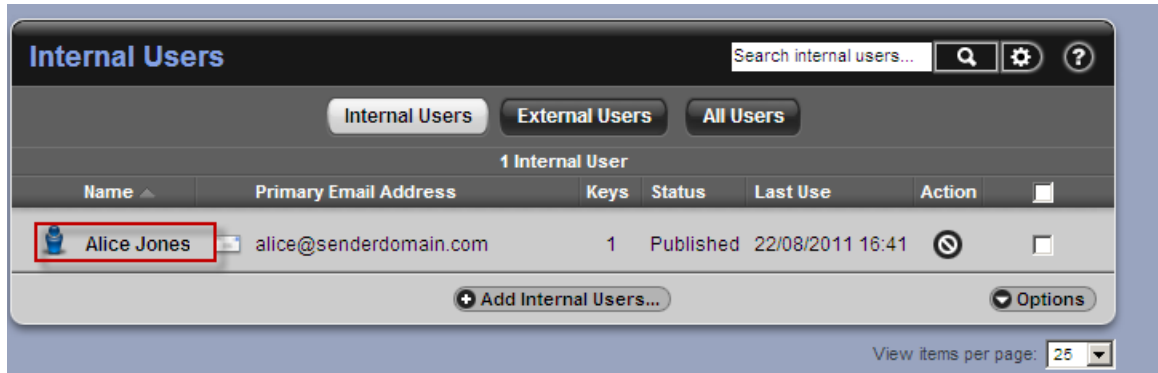
5. The computer will boot and because of the enrolment policy, the machine will pass the AD password to the OS and log in to the computer automatically. The user will be taken to their desktop where they can begin to work.

Changing Policy

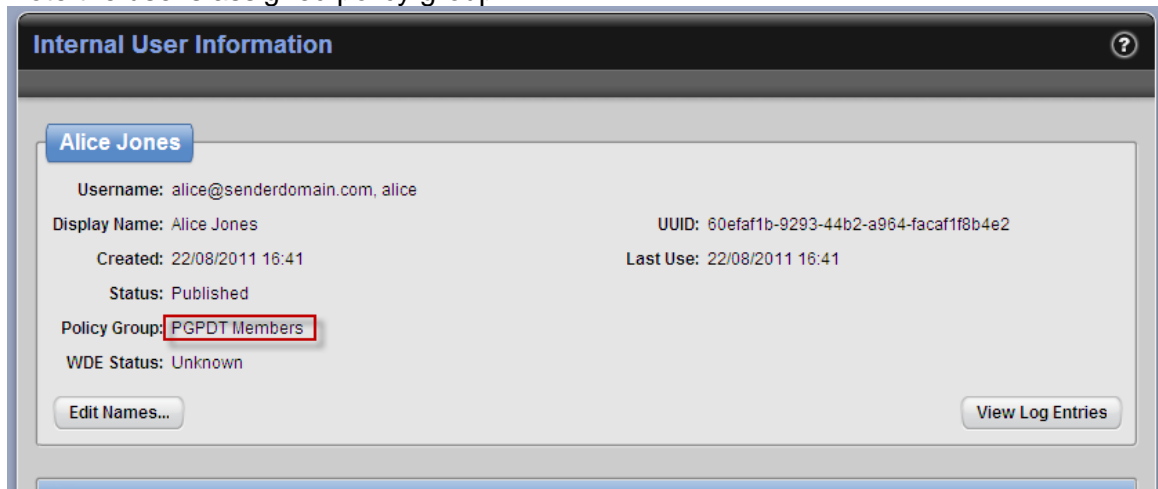
Sometimes policies and settings may need to be changed. The second part of this lab will demonstrate a policy change and how the Symantec Encryption Desktop client can be forced to update policy. Policies changes are also pulled after a specified time period (24 hours by default).

1. Go to the ***mail.senderdomain.com*** virtual machine. If prompted for a login:
 - a. Username: administrator
 - b. Password: Symc4now!
2. If the AD server asks you to reboot, choose to restart later

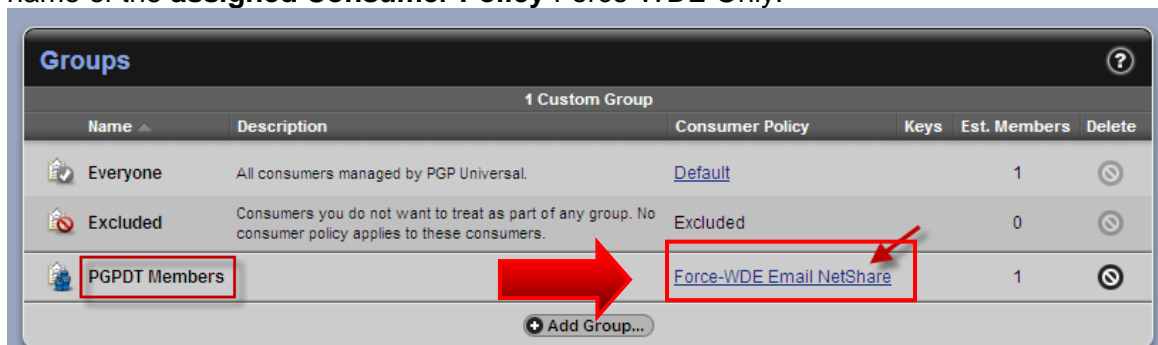
3. Open Internet Explorer and login to the Symantec Encryption Server at <https://keys.senderdomain.com:9000>
 - c. Username: admin
 - d. Passphrase: Symc4now!
4. Close any popup window that appears and go to the Consumers / Users Tab.
5. Find **alice** user and click on the name to see the user's details



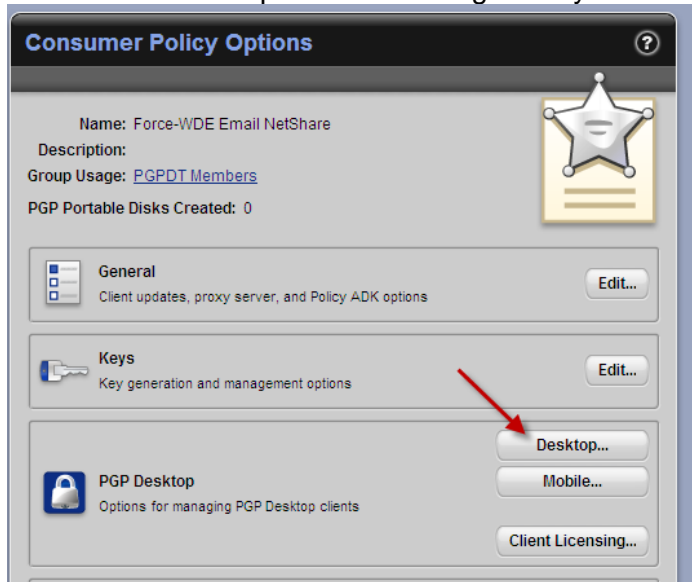
6. Note the user's assigned policy group:



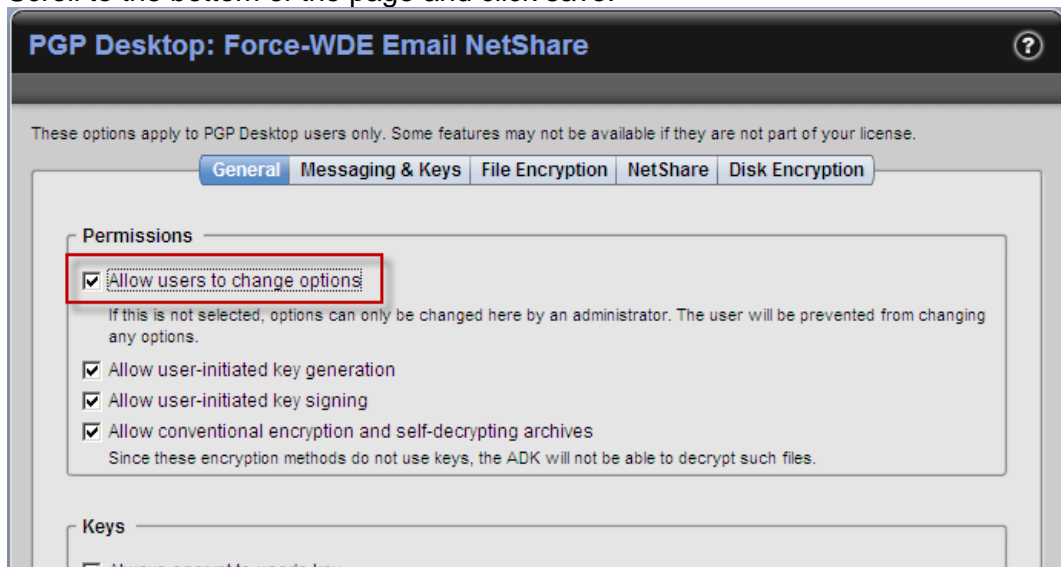
7. Go to the Consumers / Consumer Policy tab, find the Group and click on the name of the **assigned Consumer Policy Force-WDE Only**.



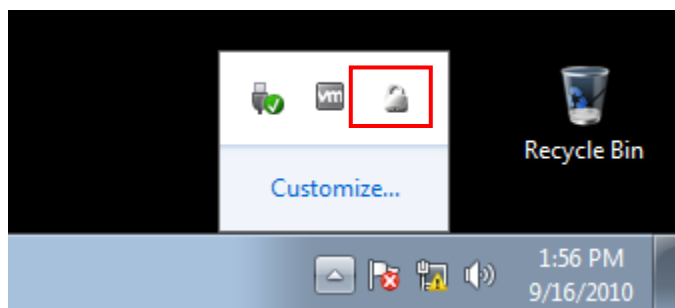
8. Click on the Desktop button to the right of Symantec Encryption Desktop.



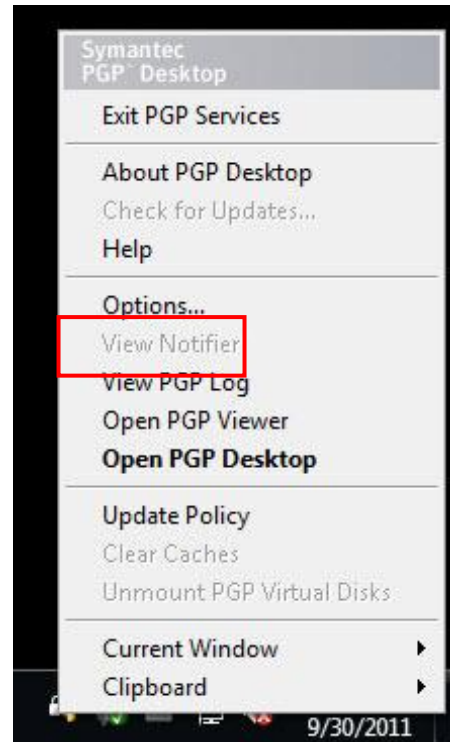
9. On the General Tab, **uncheck** the box that states *Allow users to change options*. Scroll to the bottom of the page and click save.



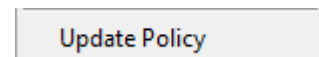
10. Switch back to the **client1** virtual machine. On the Taskbar, select the up arrow on the bottom right. This will reveal more tray icons that Windows 7 hides. If you don't see an up arrow, go straight to step 11.



11. Next right click on the Symantec Encryption Desktop lock icon to reveal the popup menu. You will notice that the **Options selection** is still **black** and can be selected by the user.



12. This is the option that was just changed on the server. However, the policy has not been updated because the policy engine only updates from the client side:
- After a configured time interval – default 24 hours
 - If a user forces update from this menu.
13. With the popup menu still visible, left click on **Update Policy**. This will force the client to retrieve the current policy from Symantec Encryption Server.
14. Once the policy update is finished, right click on the PGP Lock Icon again and you will notice that the **Options selection is now greyed out**.

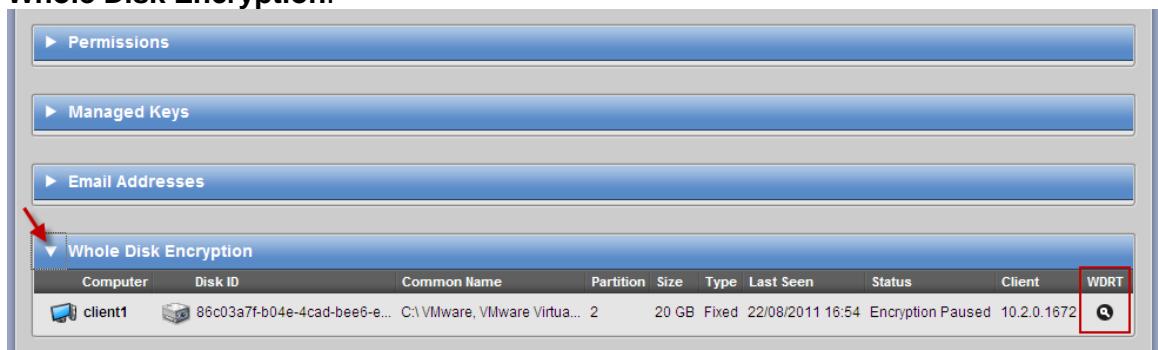


Lab Exercise 3 - Recoverability Options

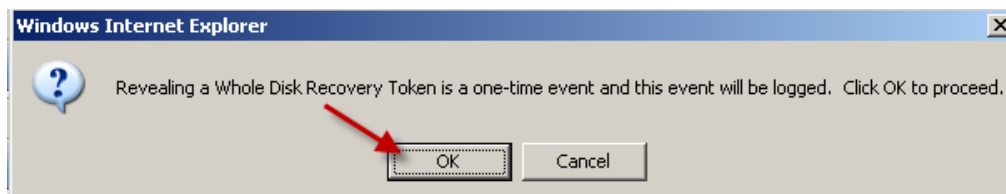
Estimated duration: 15 - 20 minutes

In the event a user forgets the Whole Disk passphrase, what can be done? This lab will do a walkthrough of using the Whole Disk Recovery Token to boot the computer to a login window.

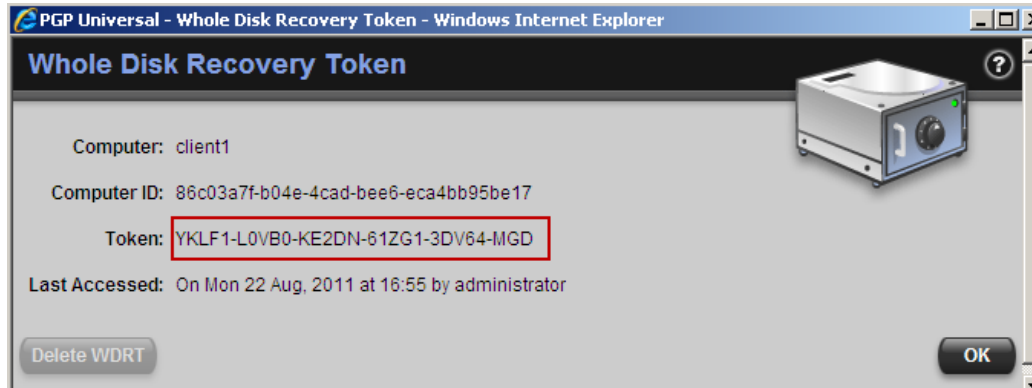
1. Lets pretend Alice forgot her password to login to Windows and the pre-boot environment.
2. Restart the client1.senderdomain.com machine and leave it waiting on the pre-boot authentication screen. This is the moment when Alice would call up helpdesk as the instructions on the pre-boot screen show.
3. The Help Desk agent now needs to reset the Windows Active Directory password and provide Alice with a Whole Disk Recovery Token, so she can login at the pre-boot screen
4. Playing the role of the Help Desk Agent, log in to the Symantec Encryption Server Administrative Interface from the **mail.senderdomain.com server** at <https://keys.senderdomain.com:9000> .
 - a. Username: admin
 - b. Passphrase: Symc4now!
5. Close the popup window (if it appears) and go to the Consumers / Users Tab.
6. Left click on the **Alice Jones** user record
7. Scroll down on the User Information Page and click on **the left arrow next to Whole Disk Encryption**.



8. On this line is the computer and disk information. Additionally, on the far right is the ability to view a Whole Disk Recovery Token. (WDRT) Click on the **magnifying glass** to begin the reveal process.
9. A warning dialog states that the action is being logged. Click the OK button to reveal the token.



10. The highlighted token is an example of a WDRT. This token (on your Symantec Encryption Server) is unique per client. This is the token that will be entered in the Symantec Encryption Desktop Pre boot environment of your enrolled Windows 7 PC. (We'll come back to this in a few minutes.)

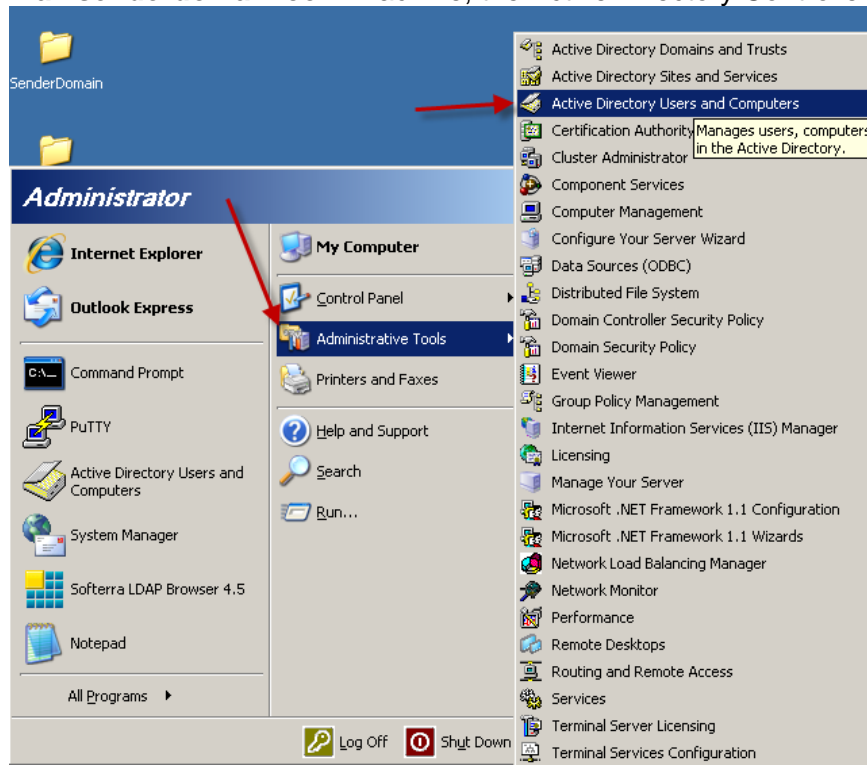


11. Write the token down for later use here:

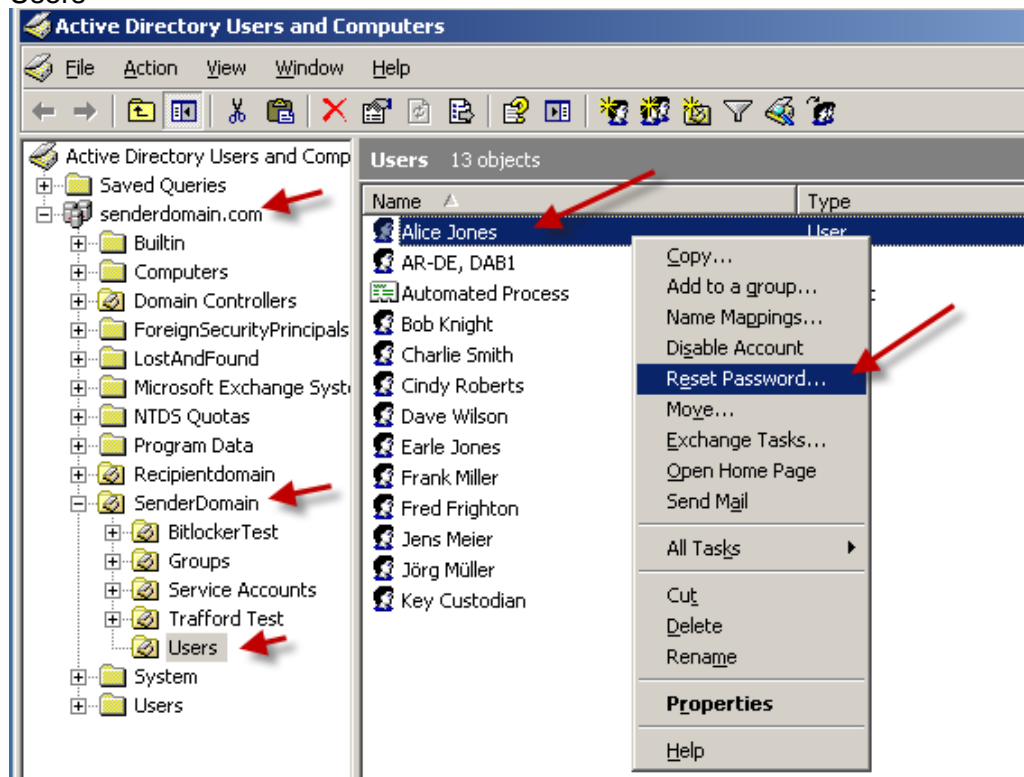
Client1 WDRT: _____

12. Close the WDRT window and log out of Symantec Encryption Server management console
13. Now, we need to reset Alice's Windows Active Directory password, so she can login to the Windows system again.

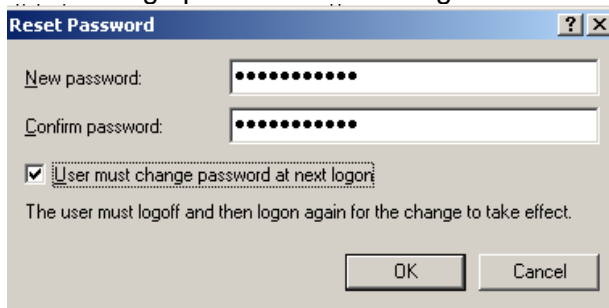
14. Still as Help Desk Agent open "Active Directory Users and Computers" on the **mail.senderdomain.com** machine, the Active Directory Controller



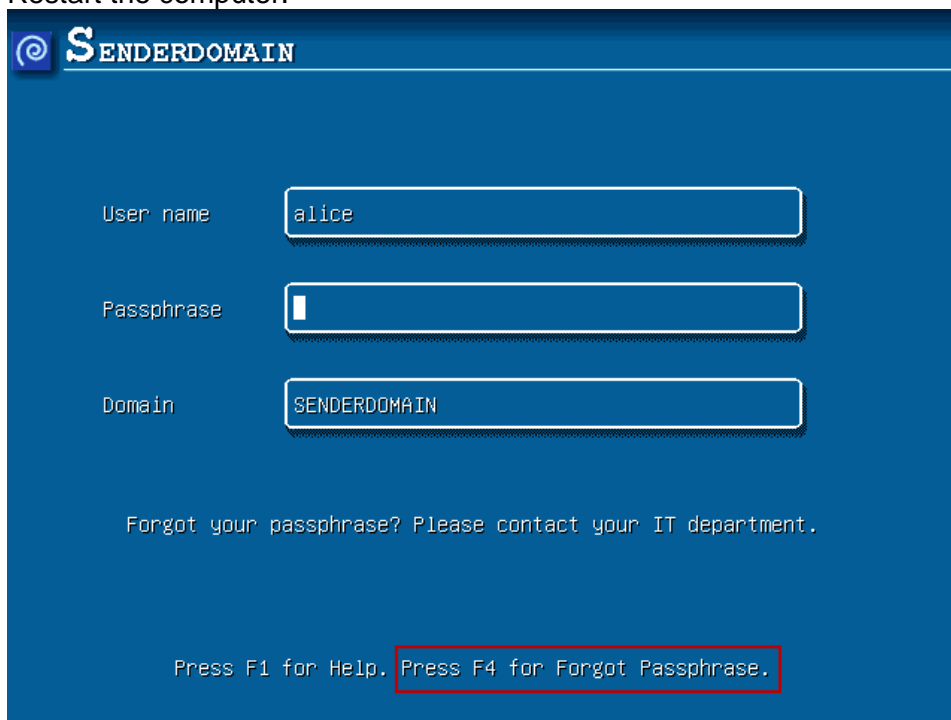
15. Locate Alice's user object in the tree under "senderdomain.com, SenderDomain, Users"



16. Right click the user object and select "Change Password"
17. Enter a new password for Alice twice (e.g. "Password123") and select "User must change password at next logon"

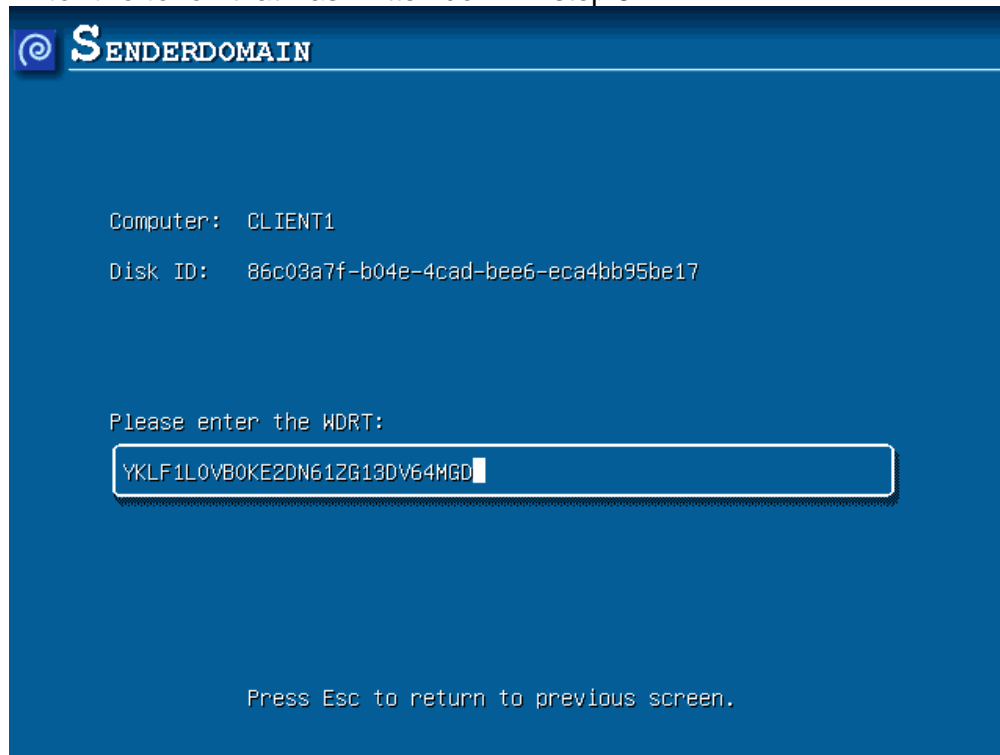


18. Now, lets go back in Alice's role and switch back to the *client1* virtual machine. Restart the computer.



19. Once the virtual machine is at the Symantec Encryption Desktop pre-boot prompt, press the **F4** key on the keyboard. This will show the screen to enter the Whole Disk Recovery Token. This screen also shows the computer name and a unique Disk ID that can be given to the Help Desk operator in case the computer cannot be otherwise identified.

20. Enter the token that was written down in step 8



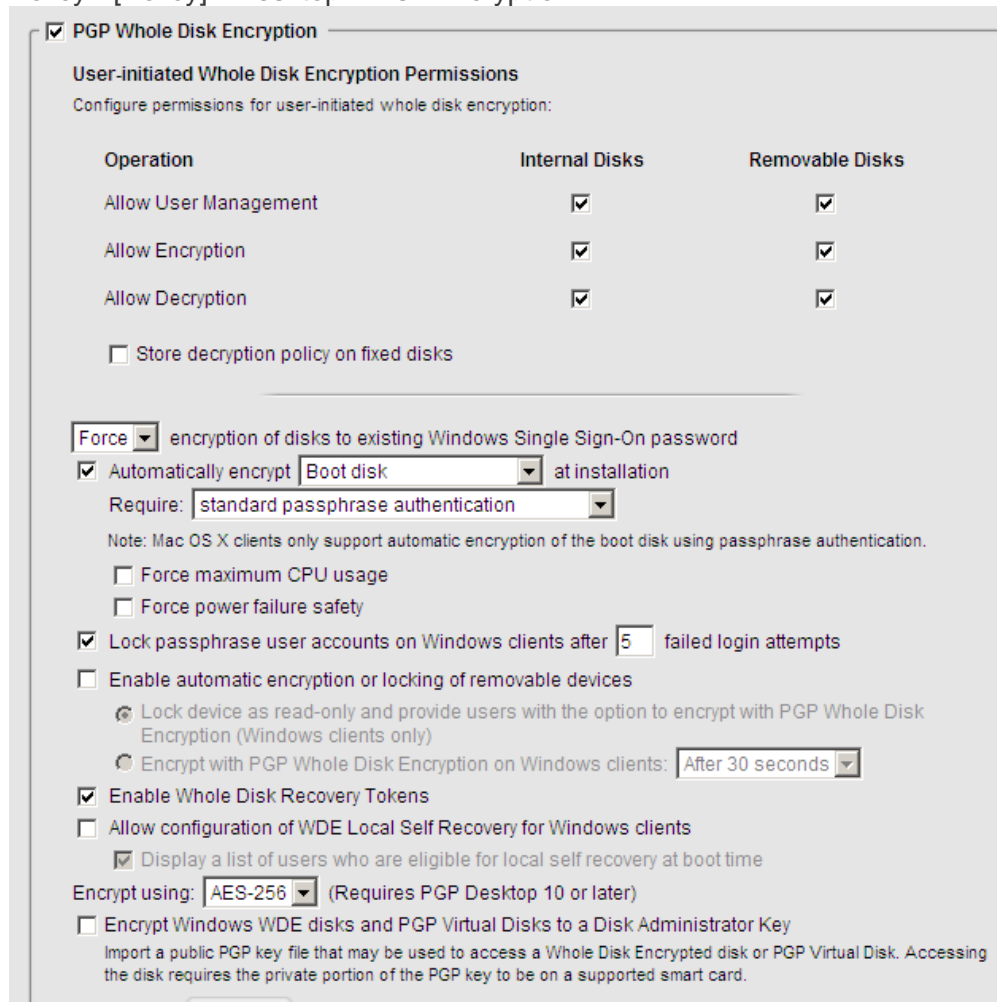
21. The token can be entered with or without the dashes and it is not case-sensitive.
22. Once the token is entered, press the **Enter** key to boot the machine.
23. The machine will boot to the login prompt where the user may now log in. In this case the user is not authenticated directly to the computer using SSO because a recovery option was used and the user's password was not entered.
24. Login as **alice** user and wait until Symantec Encryption Desktop tray service has started.
 - a. Username: alice
 - b. Password: (your new password, e.g. "Password123")
 - c. Domain: Senderdomain
25. Now Alice is prompted to reset her password, as it was changed by the Help Desk Agent. Enter a new password (e.g. "Symantec2") and finish the login.
26. The new password is now synched to the pre-boot environment and from now on Alice can use the new password to login at the pre-boot environment
27. (Optional step) Reboot **client1** machine and login again using the new password (e.g. "Symantec2")
28. Switch back to the **mail.senderdomain.com** server and the **Universal Server management console**. Check the WDRT for this disk again as described in **steps 4 to 10**. Note the token has now changed and the old token is no longer valid.

Optional Tasks:

1. **Examine encryption status** through Symantec Encryption Server management console through Consumers - Devices



2. **Examine further Desktop policy settings** through Consumers - Consumer Policy - [Policy] - Desktop - Disk Encryption



3. **Use the classic (password only) pre-boot screen.**
In the policy settings for **alice** at Consumers - Consumer Policy - [Policy] - Desktop - Disk Encryption select to use the simple pre-boot logon screen. Then update the policy on **client1** and reboot the client.

WDE BootGuard Customization

These settings will be applied to custom PGP Desktop clients generated on the [Download PGP Clients](#) screen.

Display simple authentication field
Users are only prompted to enter a passphrase, which is checked against all user accounts

Display detailed authentication fields

Remember user name

Remember domain (Windows clients only)

Set default domain (Windows clients only):

4. **Examine Group settings** through Consumers - Groups - [Group] - Group Settings

Group: PGPDT Members ?

Total Estimated Members: 1

Name: PGPDT Members
Description:
Consumer Policy: [Force-WDE Email NetShare](#)

Users View...
Users imported and grouped by the administrator

Managed Devices View...
Devices grouped by the administrator

Matched Consumers View...
Consumers defined by domain, dictionary, type, and directory rules

Permissions View...
Actions that members of this group may perform

Keys View...
Group keys applied to members of this group

Group Settings...

Lab Layout

Mail Senderdomain AD and Exchange Server

Server Name: mail.senderdomain.com
Server OS: Microsoft Windows 2003 R2 Server SP 2
Server IP Address: 169.254.128.125
Username / Password: administrator / Symc4now!
Services: AD, DNS, Exchange, SMTP, CA (certificate authority)
VMWARE Network: VMNet4

Symantec Encryption Server

Server Name: keys.senderdomain.com
Server OS: Symantec Encryption Server - PGP Universal Proprietary OS (Software Appliance) 3.2
Server IP Address: 169.254.128.122
Username / Password: admin / Symc4now!
accessed from the browser of the AD Server at <https://keys.senderdomain.com:9000>
Services: Symantec Encryption Server 3.2
VMWARE Network: VMNet4

Clients

Client Name: client1.senderdomain.com
Client OS: Windows 7 64 Bit
Client IP Address: 169.254.128.123
Username / Password:
Local Admin: administrator / Symc4now!
Domain User: alice / Symantec1
VMWARE Network: VMNet4

Client Name: client2.senderdomain.com
Client OS: Windows 7 64 Bit
Client IP Address: 169.254.128.124
Username / Password:
Local Admin: administrator / Symc4now!
Domain User: bob / Symantec1
VMWARE Network: VMNet4