DASS CORPORATION

# TÀI LIỆU HƯỚNG DẪN TRIỂN KHAI SOPHOS ENDPOINT PROTECTION

## Sophos Enterprise Console & Endpoint Protection

**Giảng Hán Phú**

**6/25/2013**

Hướng dẫn cài đặt chi tiết theo từng bước

# Nội dung


1 GIỚI THIỆU ..... 2
2 TÀI LIỆU THAM KHẢO ..... 2
3 BƯỚC THỰC HIỆN ..... 3
4 CÀI ĐẶT CHI TIẾT ..... 3
4.1 TẢI PHẦN MỀM ..... 3
4.1.1 Trường hợp có license ..... 3
4.1.2 Trường hợp sử dụng trial license ..... 5
4.2 KIỂM TRA YÊU CẦU HỆ THỐNG ..... 5
4.3 CHUẨN BỊ CÀI ĐẶT ..... 7
4.4 TẠO TÀI KHOẢN ..... 8
4.5 CÀI ĐẶT SOPHOS ENTERPRISE CONSOLE ..... 9
5 QUẢN TRỊ VÀ TRIỂN KHAI ENDPOINT ..... 20
5.1 MỞ PHẦN MỀM SOPHOS ENTERPRISE CONSOLE ..... 20
5.2 DISCOVERY COMPUTER ..... 25
6 BACKUP – RESTORE ..... 26
7 TẠO GÓI CÀI ĐẶT BẰNG DEPLOYMENTPACKAGE.EXE ..... 28

# 1 GIỚI THIỆU

Tài liệu này hướng dẫn cài đặt phần mềm Sophos để bảo vệ các máy trạm, máy chủ của hệ thống.

**Phần mềm sẽ cài đặt:**

- **Sophos Enterprise Console**: Phần mềm quản trị tập trung
- **Sophos protection software**: Phần mềm dành cho máy trạm bao gồm cả máy chủ.
- **Sophos Encryption Software**: Phần mềm mã hóa full-disk nếu bao gồm trong license

**Các gói sản phẩm của Sophos tương ứng**

- Sophos Anti-virus Business
- Sophos Endpoint Protection Business
- Sophos Endpoint Protection Advanced
- Sophos EndUser Protection
- Sophos EndUser Data Suite
- Sophos EndUser Web Suite
- Sophos Complete Security Suite

# 2 TÀI LIỆU THAM KHẢO

Dot NET Framework 4.0

http://www.microsoft.com/en-us/download/details.aspx?id=24872

Enterprise Console: IP address discovery

http://www.sophos.com/en-us/support/knowledgebase/16436.aspx

Discovery Computer fail

http://www.sophos.com/en-us/support/knowledgebase/54314.aspx

Hướng dẫn tạo Account:

http://www.sophos.com/en-us/support/knowledgebase/113954.aspx

Hướng dẫn backup restore: DataBackupRestore

http://www.sophos.com/en-us/support/knowledgebase/114299.aspx

# 3 BƯỚC THỰC HIỆN

- Tải phần mềm Enterprise Console.
- Kiểm tra yêu cầu hệ thống.
- Tạo tài khoản trên Windows nếu cần.
- Chuẩn bị cài đặt.
- Cài đặt Enterprise Console.
- Tải phần mềm Protection và Encryption.
- Tạo các nhóm.
- Thiết lập chính sách bảo mật.
- Tìm kiếm máy tính.
- Chuẩn bị cài đặt lên máy trạm.
- Cài đặt lên máy trạm.
- Cài đặt phần mềm mã hóa nếu có (phụ thuộc license).
- Kiểm tra tình trạng của mạng.

# 4 CÀI ĐẶT CHI TIẾT

## 4.1 TẢI PHẦN MỀM

### 4.1.1 Trường hợp có license

Các điểm lưu ý trong license như sau:

- Start Date: thời gian license được active (hoạt động).
    - Nếu ngày đang cài đặt chưa đến ngày Start Date thì lúc nhập Username/Password của license vào phần mềm sẽ không được. Trường hợp này nên sử dụng license Trial 1 tháng trước.
- Expiry Date: Thời gian license hết hạn
- Username: Tài khoản dùng để download phần mềm và bản cập nhật từ Sophos ngay chính trong phần mềm
- Password: Mật khẩu cần để nhập.

| LICENSE NUMBER | QUANTITY | PRODUCT | TYPE | START DATE | EXPIRY DATE |
|---|---|---|---|---|---|
| L0000[redacted] | 100 | Endpoint Protection - Business - Competitive Upgrade | Subscription | 14/[redacted]2013 | 13/[redacted]2014 |

Credentials:

| LICENSE NUMBER | PRODUCT | USERNAME | PASSWORD |
|---|---|---|---|
| L0000[redacted] | Endpoint Protection - Business - Competitive Upgrade | [redacted] | [redacted]7jo |

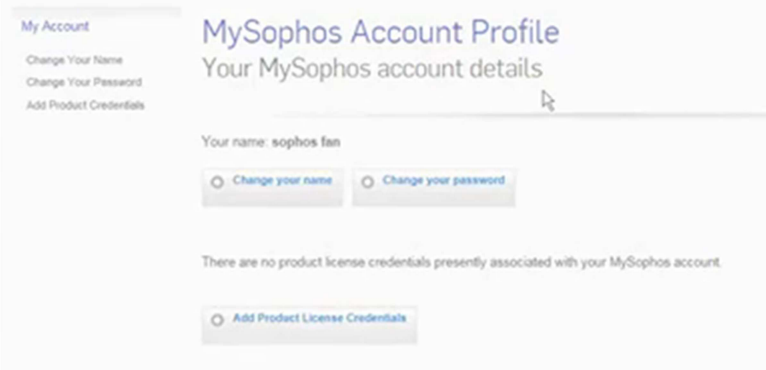
Để tải được phần mềm, người quản trị cần tạo một tài khoản tại website của Sophos.

- Tài liệu hướng dẫn từ Sophos: http://www.sophos.com/en-us/support/knowledgebase/111195.aspx
- Video hướng dẫn đăng ký: http://www.youtube.com/watch?v=mtN9p6BSpNI#!

#### *4.1.1.1 Hướng dẫn tạo tài khoản step-by-step:*

- Vào link đăng ký: https://secure2.sophos.com/en-us/mysophos/registration.aspx
- Điền thông tin: Email, Tên, họ, mật khẩu

- Bấm "Continue": Một email active tài khoản sẽ gửi đến Email của người quản trị
- Kiểm tra email và click vào link active tài khoản
- Login vào tài khoản bằng link: https://secure2.sophos.com/en-us/mysophos/login.aspx (có thể tìm link ở trang chủ Sophos.com, ở giữa, phía trên cùng)
- Vào Account Profile sau khi login, Click nút "Add Product License Credentials"




- Nhập Username và Password từ LICENSE phía trên vào
- Lúc này người quản trị có thể download phần mềm từ link sau (có thể thấy trong menu Support – Updates/Download): http://www.sophos.com/en-us/Sophos/Support/Downloads.aspx

#### *4.1.1.2 Các phần mềm cần tải*

- **Sophos Enterprise Console (sec_521_sfx.exe)**: Phần mềm quản trị, phiên bản 5.x
- **Sophos Deployment Packager (sdp_121_sfx.exe)**: Phần mềm để tạo gói cài đặt cho máy trạm
- **PureMessage for Microsoft Exchange**: Phần mềm Anti-virus/Anti-spam cho Microsoft Exchange
- **Safeguard Private Crypto**: Phần mềm mã hóa file cho người dùng cuối

### 4.1.2 Trường hợp sử dụng trial license

Link trial: www.sophos.com/en-us/products/free-trials/endpoint-protection.aspx

Điền thông tin theo form và sẽ nhận được tài khoản trial 1 tháng cùng với link download qua email.

## 4.2 KIỂM TRA YÊU CẦU HỆ THỐNG

Kiểm tra thông tin mới nhất tại website Sophos:

http://www.sophos.com/en-us/support/knowledgebase/118620.aspx

**Endpoint Protection**

- Sophos Anti-Virus for Windows
- Sophos Client Firewall
- Sophos Anti-Virus for Mac

- Sophos Anti-Virus for Linux
- Sophos Anti-Virus for UNIX
- Sophos Anti-Virus for Network Storage
- Sophos for Microsoft SharePoint
- Enterprise Console

Sophos Enterprise Console System Requirements

| Platforms supported | x86 32-bit | x86 64-bit | IA-64 (Itanium) 64-bit | Minimum memory | Minimum disk space |
|---|---|---|---|---|---|
| **Management server** | | | | 1 GB / 2 GB* | 500 MB / 3 GB* |
| Windows 7** | ✓ | ✓ | | | |
| Windows SBS 2011** | | ✓ | | | |
| Windows Server 2008* | ✓ | ✓ | | | |
| Windows Server 2008 R2* | | ✓ | | | |
| Windows Server 2003 and R2* | ✓ | ✓ | | | |
| **Remote console** | | | | | |
| Windows 7 (including XP mode) | ✓ | ✓ | | | |
| Windows SBS 2011 | | ✓ | | | |
| Windows Server 2008 | ✓ | ✓ | | | |
| Windows Server 2008 R2 | | ✓ | | | |
| Windows Server 2003 and R2 | ✓ | ✓ | | | |
| Windows Vista SP2 | ✓ | ✓ | | | |
| Windows XP Pro SP3 | ✓ | ✓ | | | |
| **Virtualization platforms supported** | | | | | |
| vSphere | | | | | |
| VMWare ESX/ESXi | | | | | |
| VMWare Workstation | | | | | |
| VMWare Server | | | | | |
| Hyper-V 2008 | | | | | |
| Citrix XenServer | | | | | |
| **Database support** | | | | | **Maximum disk space** |
| SQL 2005, 2008, 2012*** | ✓ | ✓ | | | No limit |
| SQL 2005 Express Edition | ✓ | ✓ | | | 4 GB |
| SQL 2008 Express Edition | ✓ | ✓ | | | 4 GB |
| SQL 2012 Express Edition*** | ✓ | ✓ | | | 10 GB |
| **Platforms managed** | | | | | |

| |
|---|
| • Windows, Mac OS X, Linux, Solaris 9, 10 and 11 on SPARC and Intel (i386)<br>• HP-UX on Itanium 2<br>• AIX 5.3, 6.1, and 7.1 on PowerPC |
| **Hardware** |
| 2.0 GHz Pentium or equivalent |
| **Languages supported** |
| English, French, German, Japanese, Italian, Spanish, Simplified Chinese and Traditional Chinese |

**Notes**

*** Database components from Sophos Enterprise Console 5.2 and above are supported on SQL 2012 and SQL Express 2012. Earlier versions of Enterprise Console are not supported on this version of SQL.

** Not supported by the NAC Management server

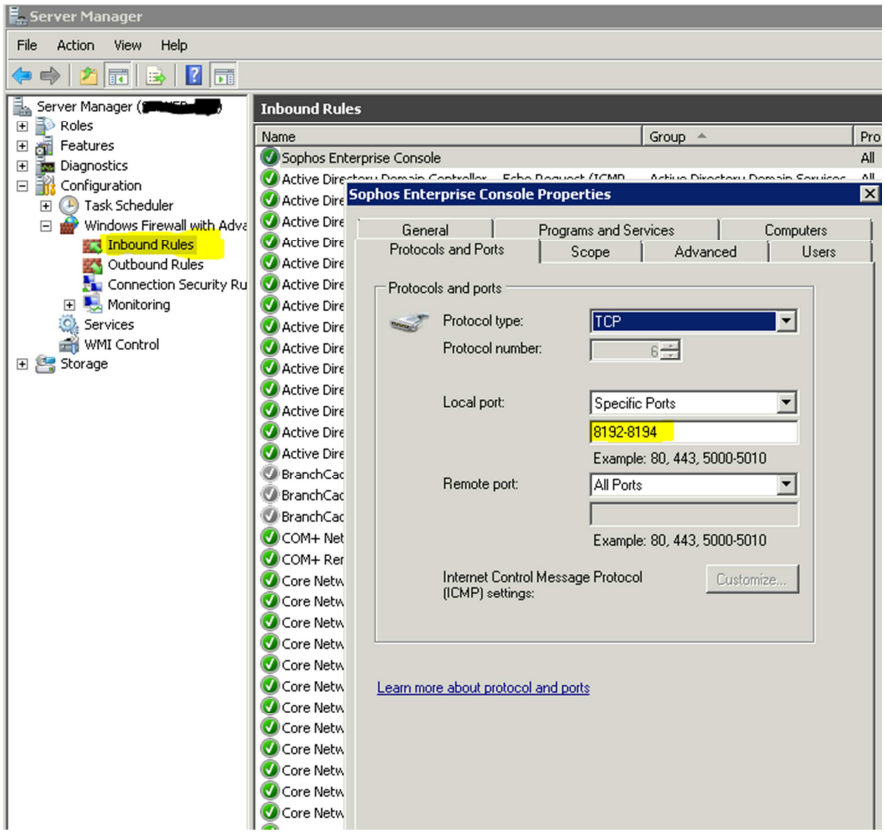
* Additional memory and disk capacity required for installation of NAC Manager

## 4.3 CHUẨN BỊ CÀI ĐẶT

- Cài .NET Framework 4.0 (tìm và download từ Microsoft.com)
- Mở các port sau trên Windows Firewall : 8192, 8193, 8194 . Các port trên cần thiết để liên lạc giữa Console và Sophos endpoint software.
- Quá trình cài đặt sẽ tự động cài SQL Server 2008 Express (trường hợp không sử dụng SQL server riêng)
- Quá trình cài đặt sẽ tự động cài Microsoft Message Queuing (MSMQ)

**Inbound Firewall Rule**

- Inbound rules
- TCP ports: 8192, 8193, 8194
- Scope: **ANY IP ADDRESS** hoặc **Local subnet** (tùy môi trường mạng)




## 4.4 TẠO TÀI KHOẢN

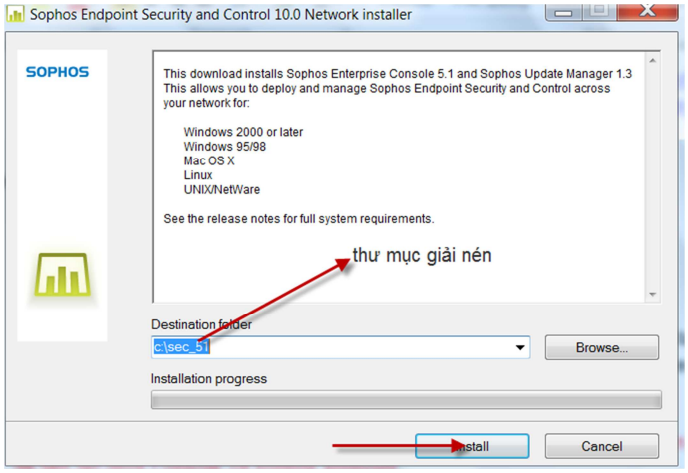
Trước khi tiến hành cài đặt, cần tạo tài khoản người dùng bằng **SERVER MANAGER** (Windows 2008/2012)

- Hướng dẫn tạo Account: http://www.sophos.com/en-us/support/knowledgebase/113954.aspx
- **Database account**: tài khoản dùng để kết nối đến database, và dùng để khởi động dịch vụ của SQL Server.
    - Password Never Expired
    - Không thay đổi sau khi cài đặt
    - Đặt tên có thể là: **SophosManagement**
    - Có thể không cần quyền Administrator.
    - Có khả năng logon vào máy chủ cài Sophos Enterprise Console
    - Có tên UPN (User Principal Name) nếu môi trường Domain
    - Có quyền ghi vào thư mục **\windows\temp**
- **Update Manager account**: tài khoản dùng để các sophos endpoint kết nối đến folder share, nơi chứa update source.
    - Password Never Expired
    - Không thay đổi sau khi cài đặt
    - Đặt tên có thể là: **SophosUpdateMgr**

- Có thể không cần quyền Administrator.
- Có tên UPN (User Principal Name) nếu môi trường Domain
- Có quyền ghi vào thư mục **\\Server-SEC\SophosUpdate** (thư mục chứa file update của Sophos Enterprise console mặc định – Server-SEC là server name)

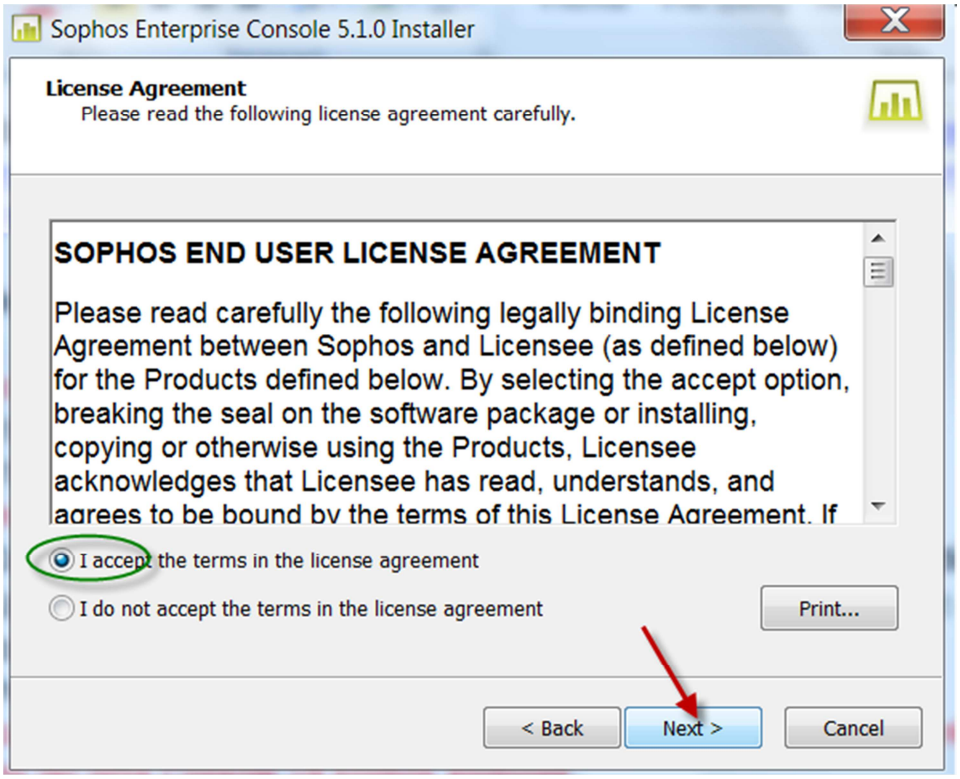
## 4.5 CÀI ĐẶT SOPHOS ENTERPRISE CONSOLE

- Đăng nhập vào máy chủ với quyền Local Admin hoặc Domain Admin.
- Click đôi vào gói cài đặt: **sec_5xx_sfx.exe**
- Màn hình cài đặt hiện ra như bên dưới



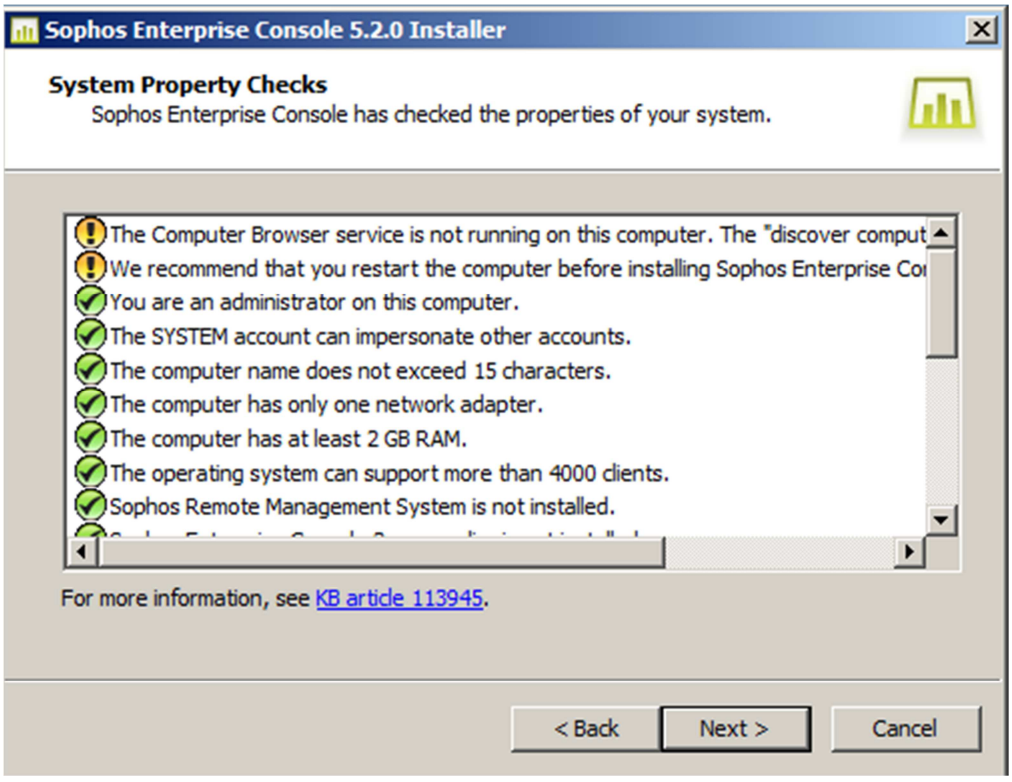

Click nút Install

Click Next




Click chọn “I accept…” và Next

Installer sẽ kiểm tra yêu cầu hệ thống, và thông báo như bảng sau:



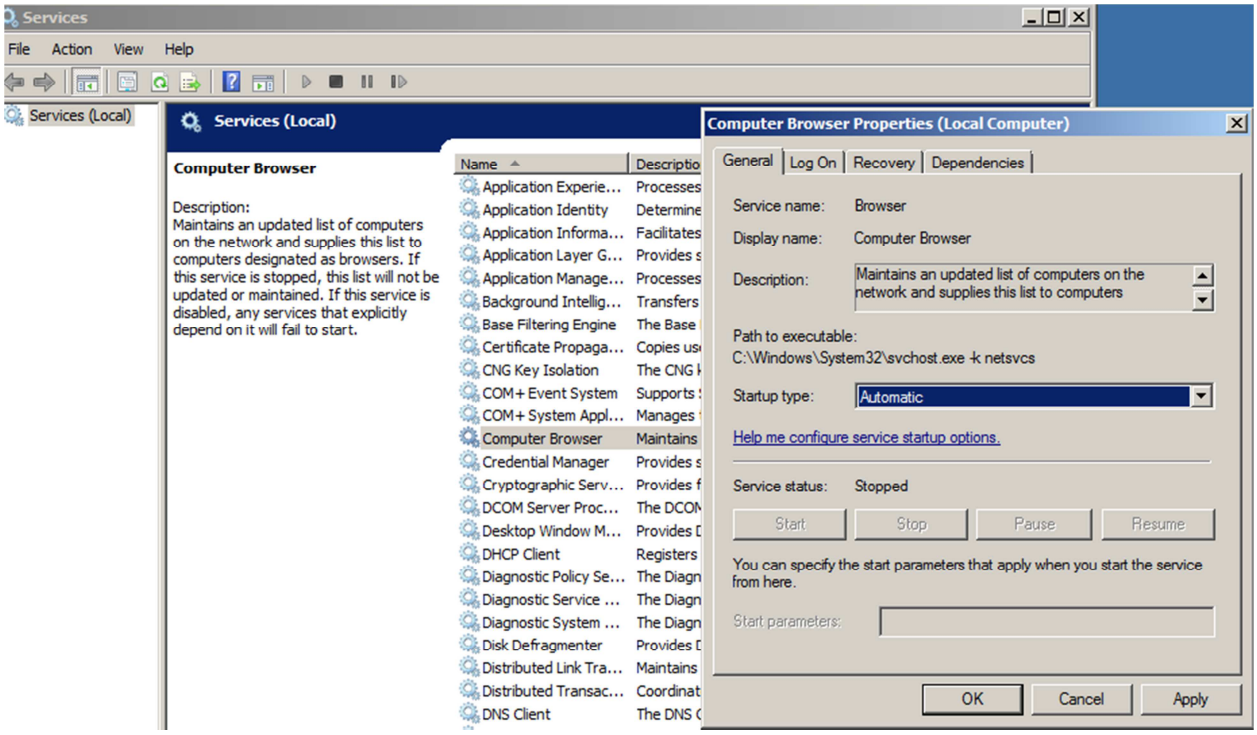
Với thông báo trên, máy chủ cần bật “Computer Browser Service” và khởi động lại trước khi cài đặt.

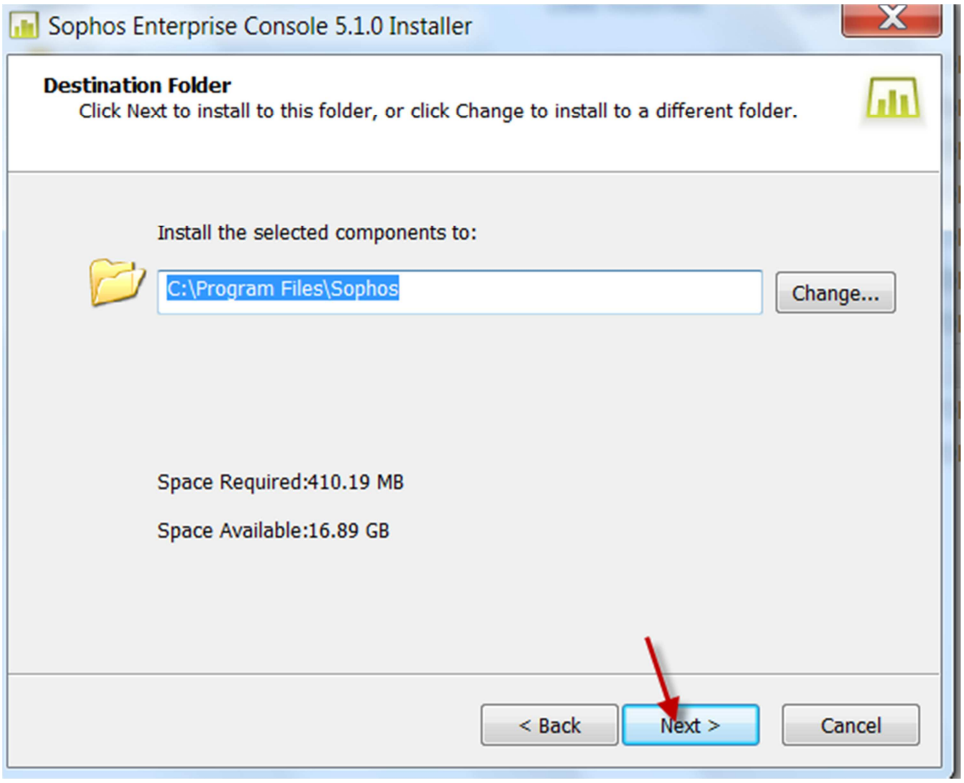
Bật “Computer Brower Service” bằng cách sau:

- Vào Administration Tools -> Services -> Computer Browser

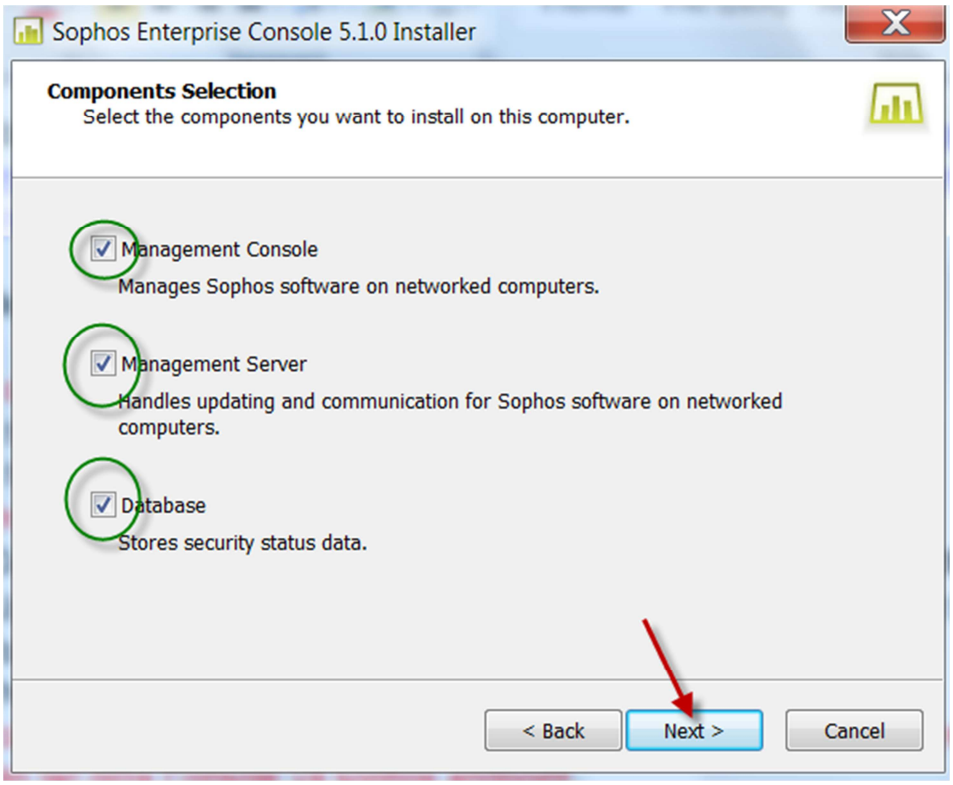
- Click phải Computer Browser Service -> Properties -> Startup Type = Automatic

- Click Apply -> Start service.

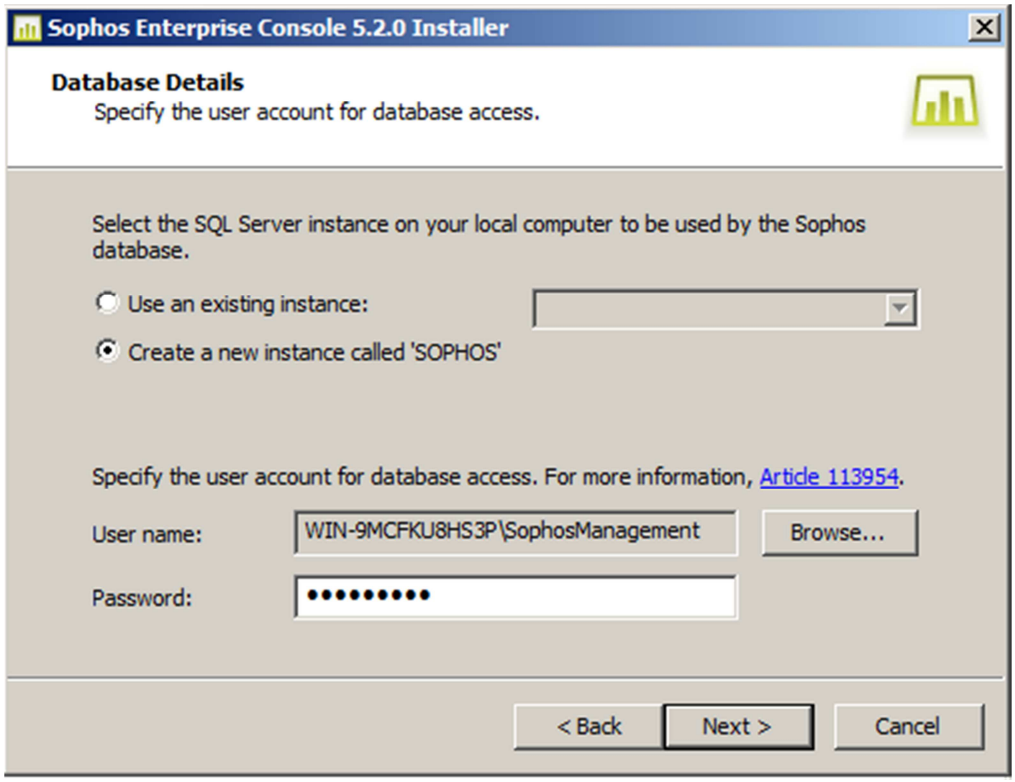





Click NEXT (chọn thư mục default của phần mềm, không nên đổi thư mục khác)



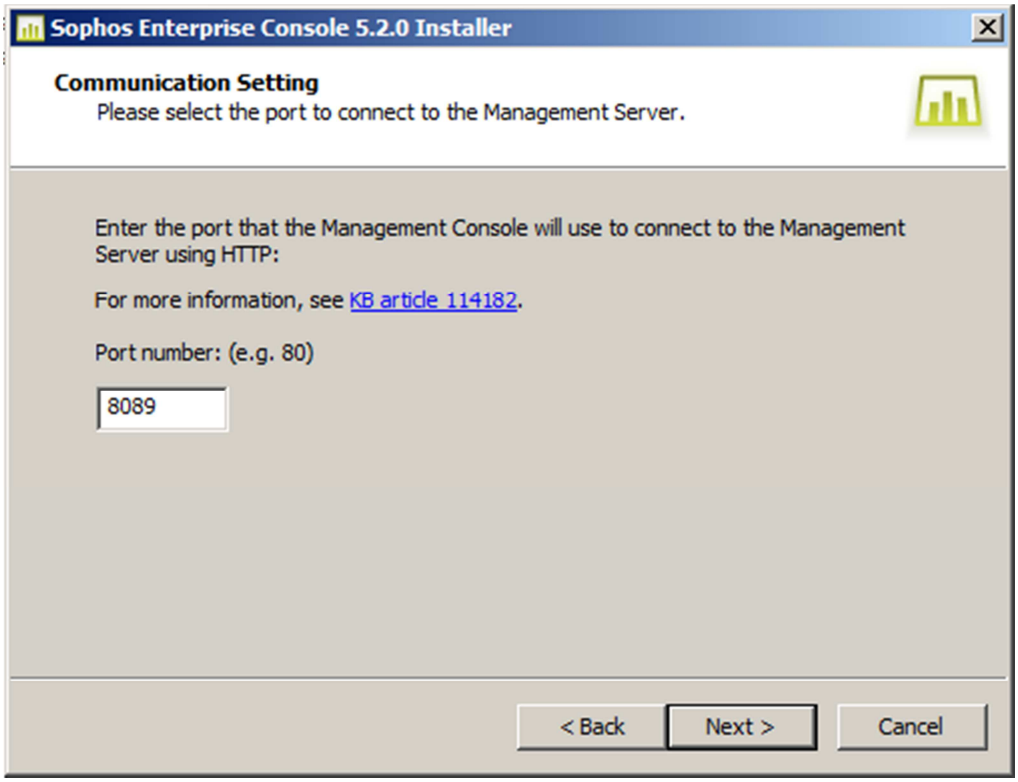

Chọn cả 3 Components. Trường hợp này SQL Server 2008 Express sẽ được cài chung nếu



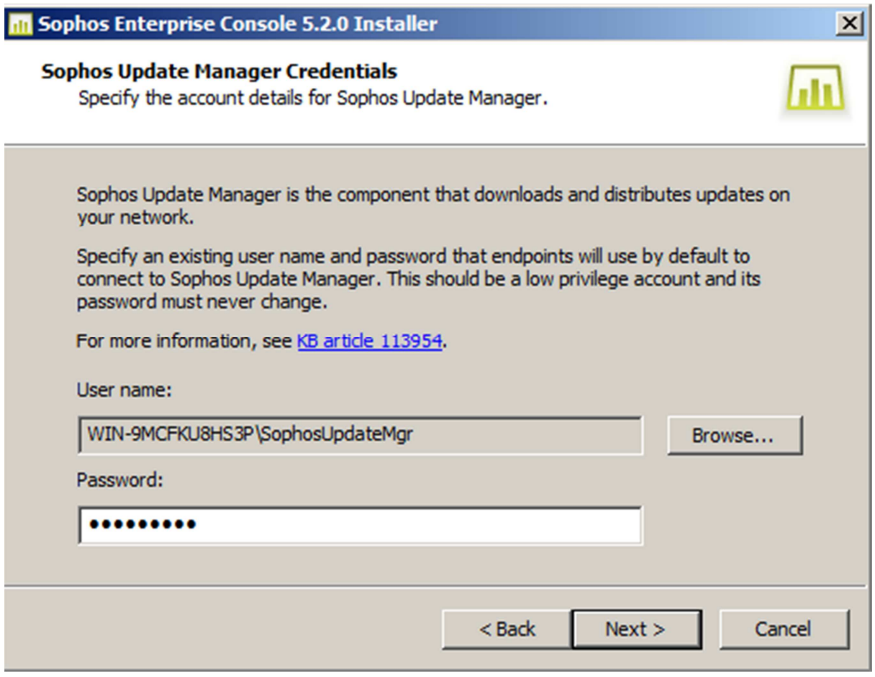

Chọn Create a new instance called ‘SOPHOS’

Click Browse… để chọn Database Account (SophosManagement đã tạo bên trên)

Click Next và chọn port 8089 làm mặc định chung.

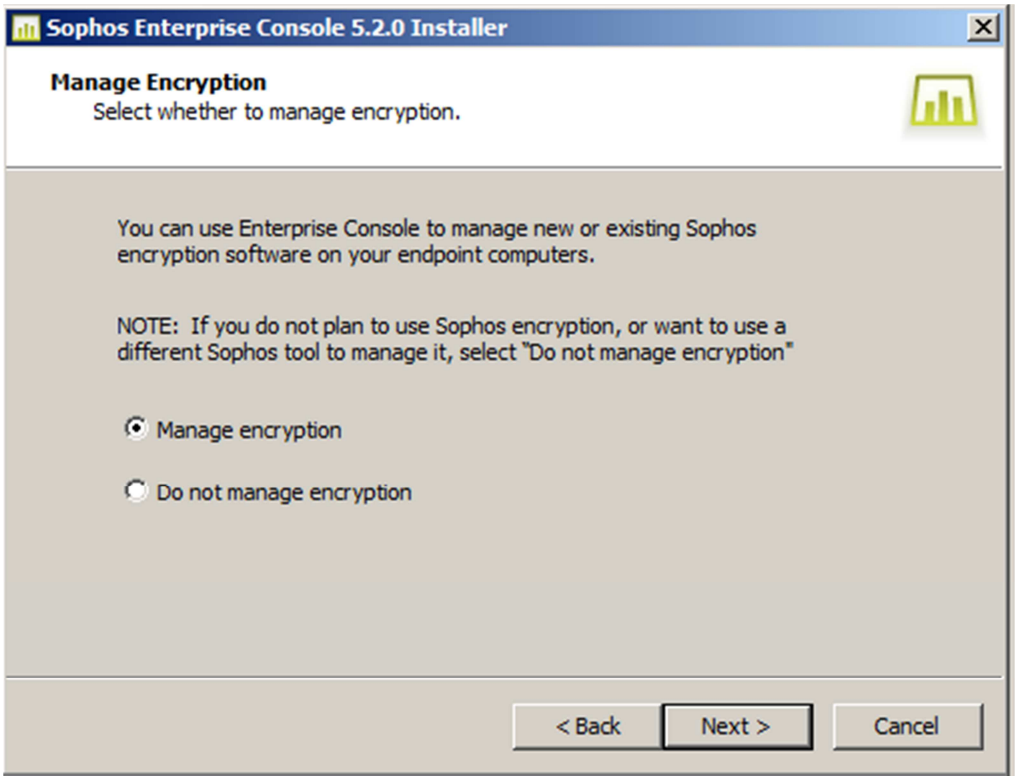



Click Next




Chọn Account dành cho Sophos Update Manager, đã tạo ở bước trước.

Click Next

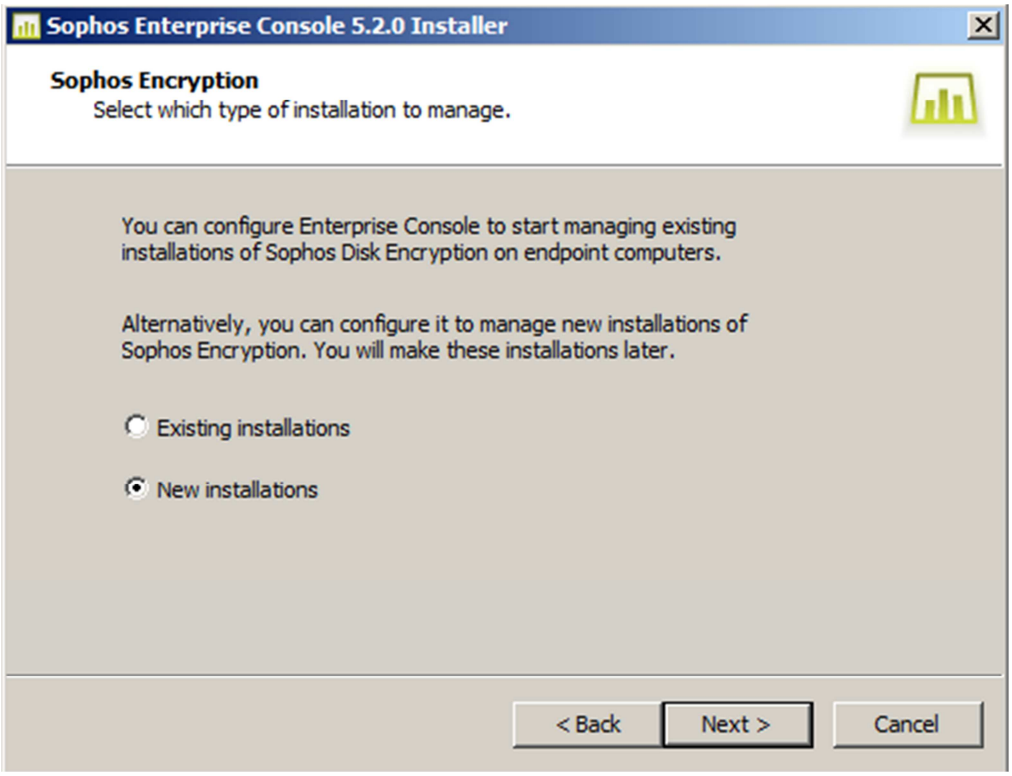



Chọn quản lý Encryption hay không. Các gói sản phẩm sau có Manage Encryption:

- Sophos EndUser Data Suite
- Sophos Complete Security Suite

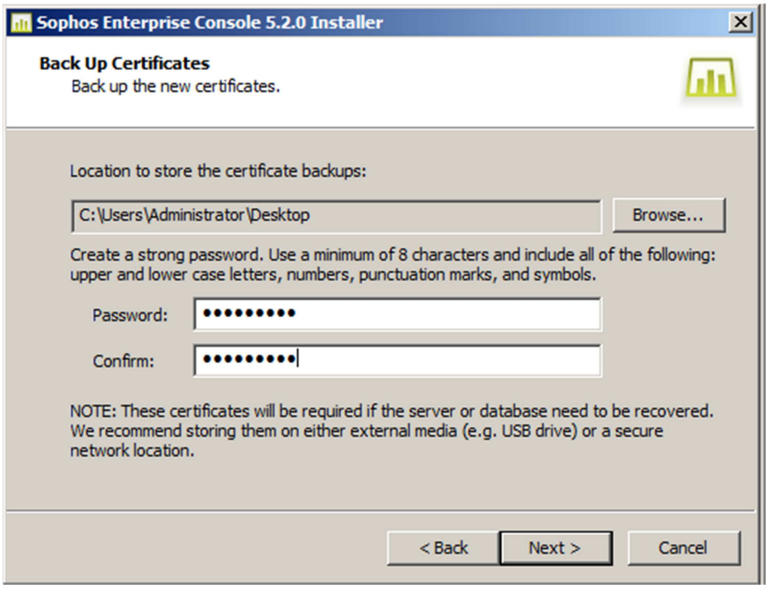
Click Next

- Nếu có Manage Encryption, lựa chọn cài mới hoặc cài nâng cấp từ version cũ.
- Chọn cài mới.



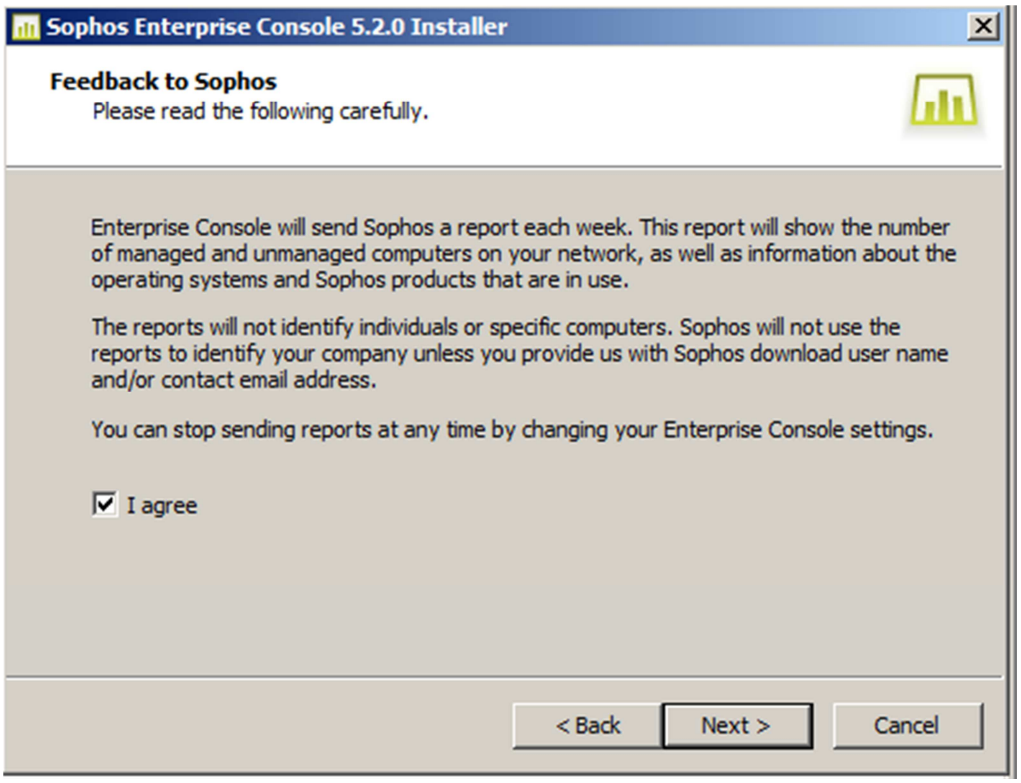

Click Next

- Chọn vị trí thư mục lưu Certificate backup (dùng cho trường hợp cài lại, restore Sophos Enterprise Console
- Đặt password cho Certificate, ghi lại password này.



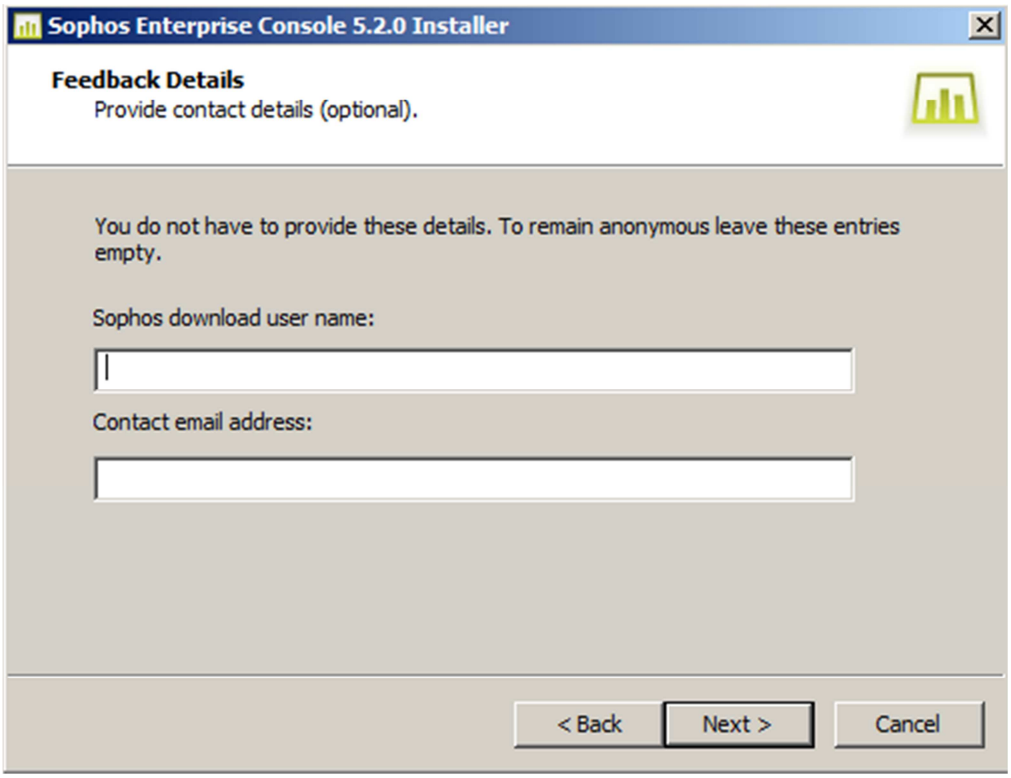

Click Next

- Lựa chọn sự đồng ý hay không việc gửi báo cáo về Sophos các số lượng máy tính đang được quản lý và không được quản lý trong hệ thống hàng tuần.
- Báo cáo này không xác định, thu thập bất kỳ thông tin của máy tính nào.
- Sophos không dùng báo cáo này để xác định công ty của khách hàng trừ khi khách hàng yêu cầu và gửi thông tin tài khoản download / hay email liên hệ
- Việc gửi report có thể ngừng lại bất kỳ lúc nào trong phần setting của phần mềm Sophos Enterprise Console

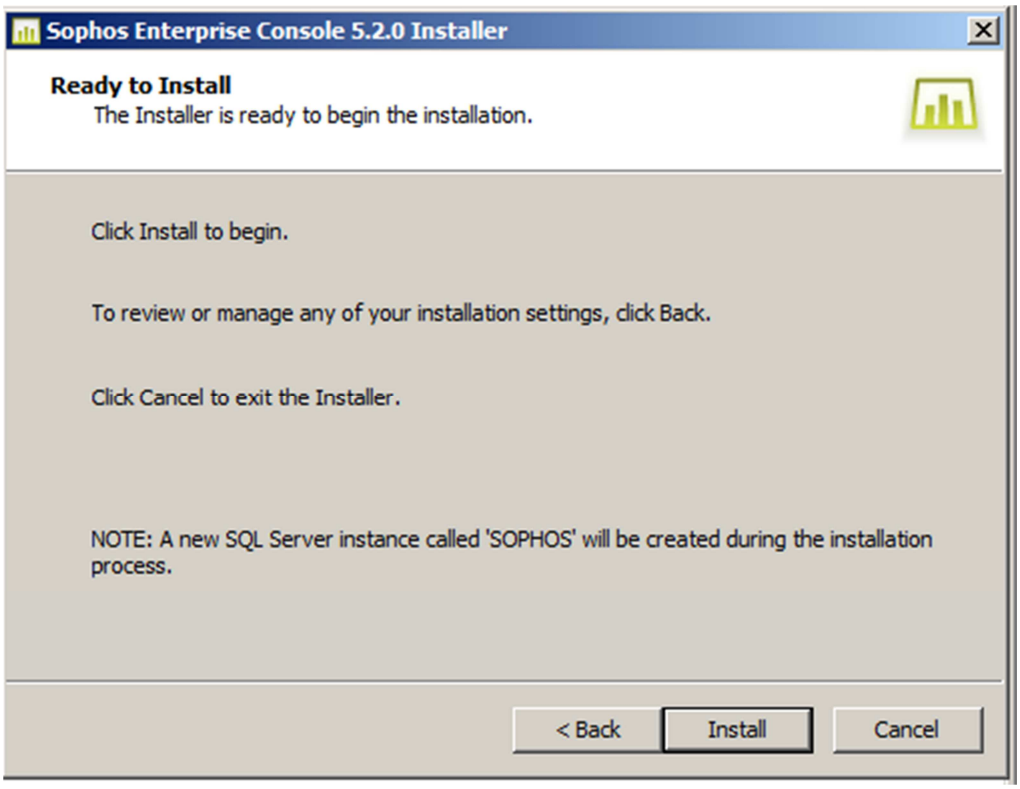



Chọn “I agree” (không bắt buột) và click Next

- Nhập thông tin tài khoản download (trong license file, hoặc trial account)
- Có thể để trống, không cần nhập, và sẽ nhập sau.

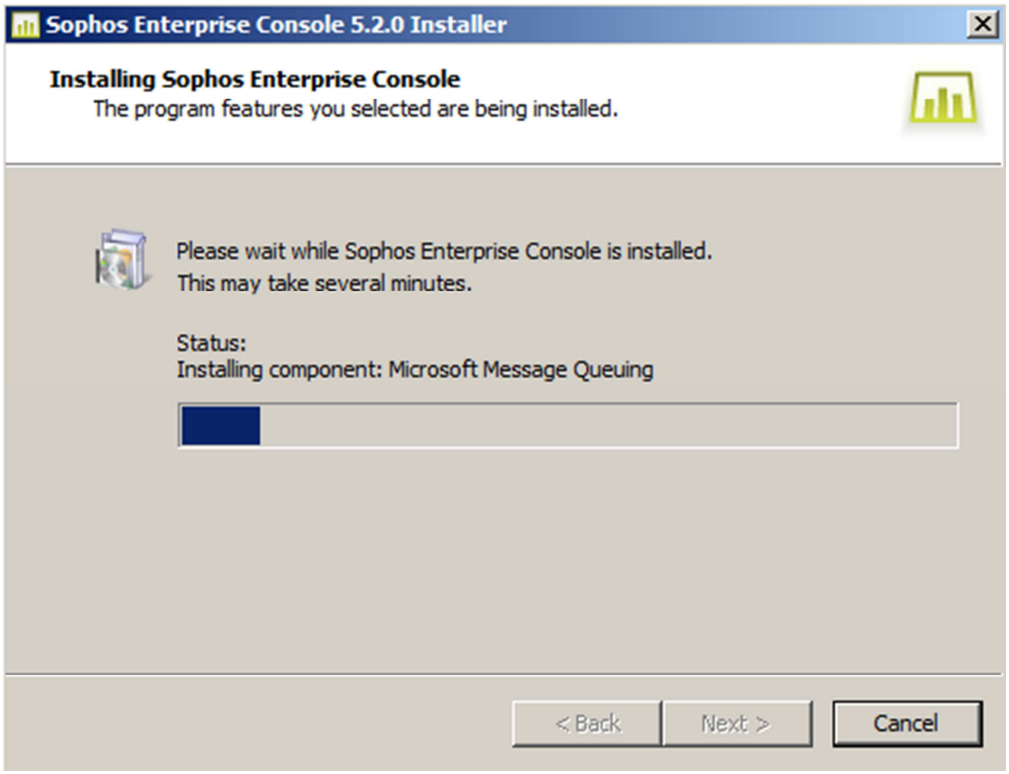



Click Next



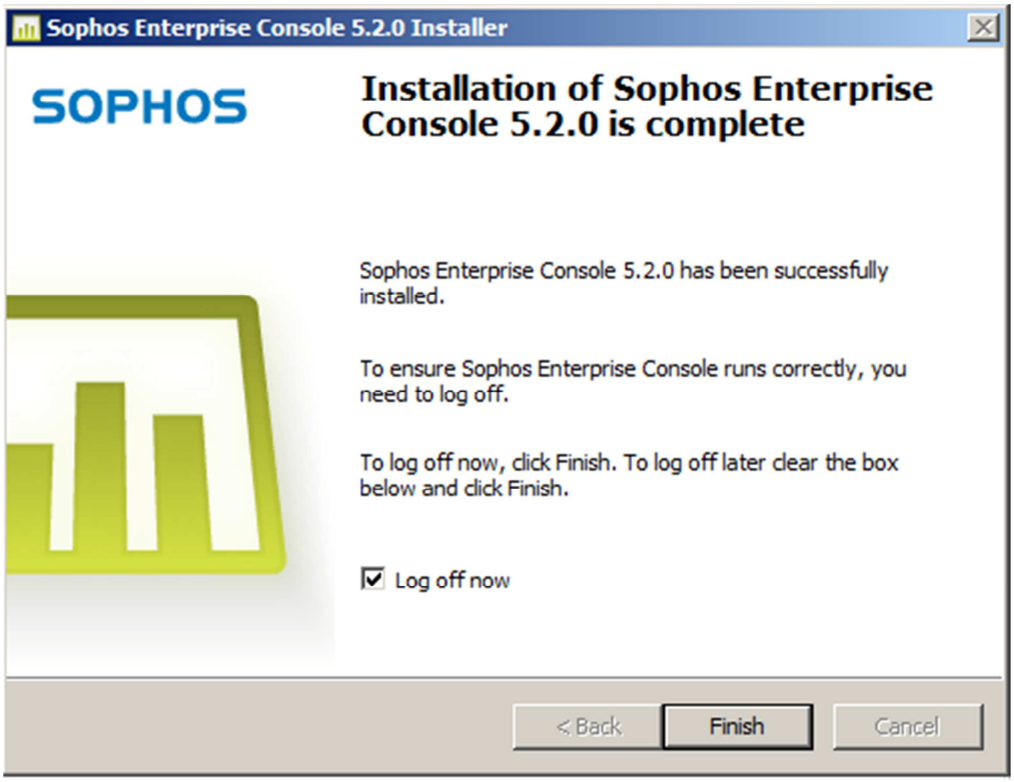

Click Install và theo dõi quá trình cài đặt. Mặc định một số gói được cài như sau

- Microsoft Message Queuing
- .NET Framework 4.0
- SQL Server 2008 R2 SP1 (Express)




Sau khi cài đặt thành công, phần mềm yêu cầu log off máy chủ.

Click Finish với tùy chọn “Log Off Now”




Kết thúc quá trình cài đặt Sophos Enterprise Console.

# 5 QUẢN TRỊ VÀ TRIỂN KHAI ENDPOINT

## 5.1 MỞ PHẦN MỀM SOPHOS ENTERPRISE CONSOLE

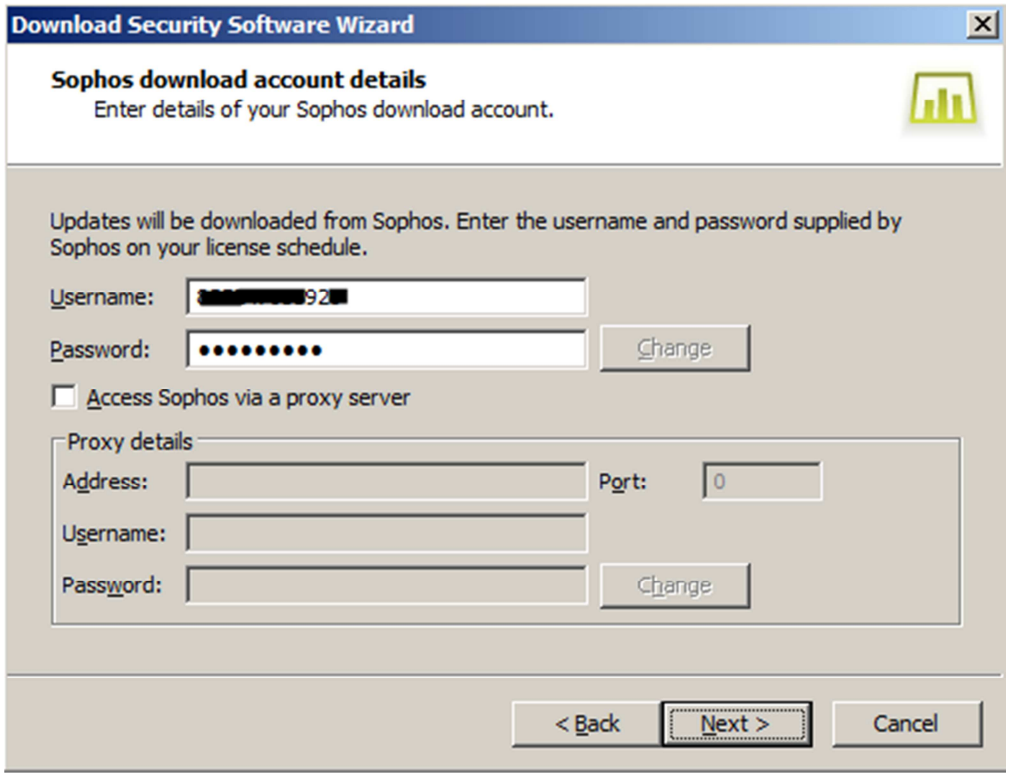
Đăng nhập vào máy chủ Sophos Enterprise Console

Mở phần mềm Sophos Enterprise Console:

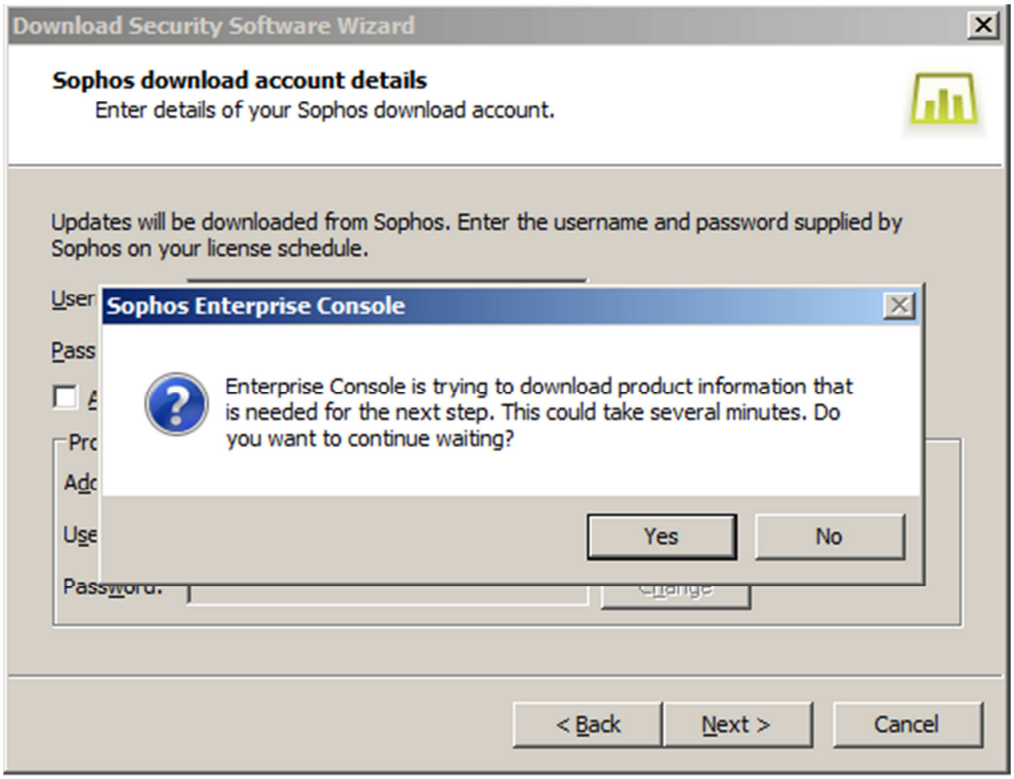
- Start -> All Programs -> Sophos -> Enterprise Console

Sau khi mở phần mềm, nếu bước nhập User/Pass download lúc cài đặt được để trống thì quá trình Download Security Software Winzard được hiển thị như sau

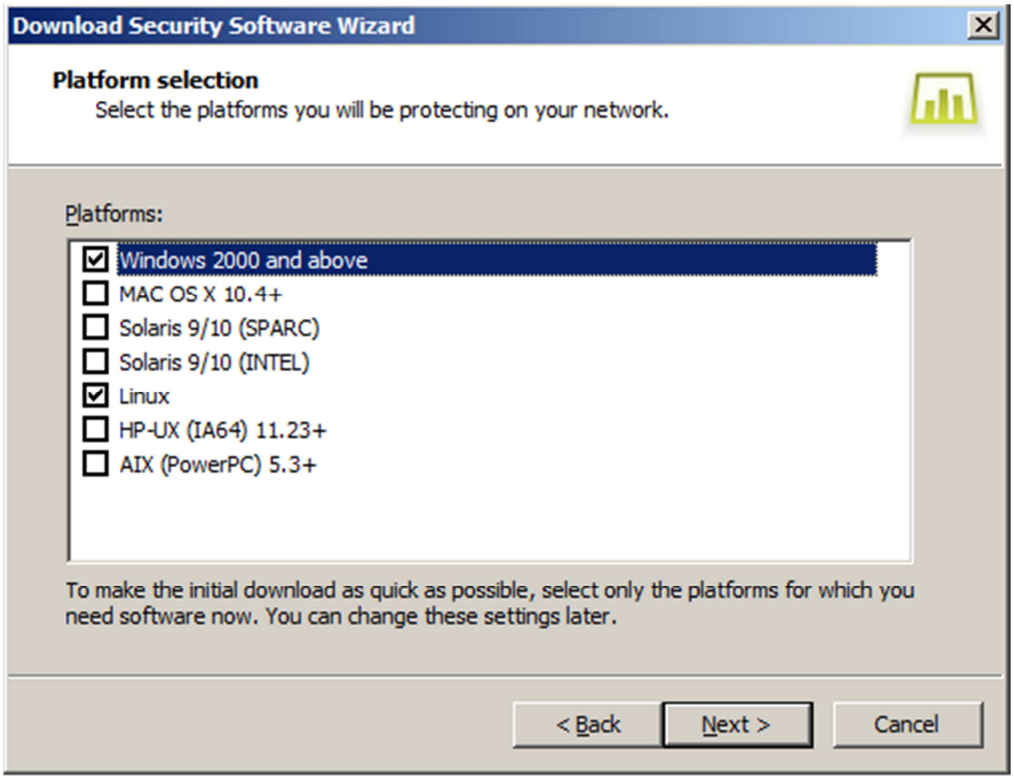
Click Next




Nhập User/Pass download của License

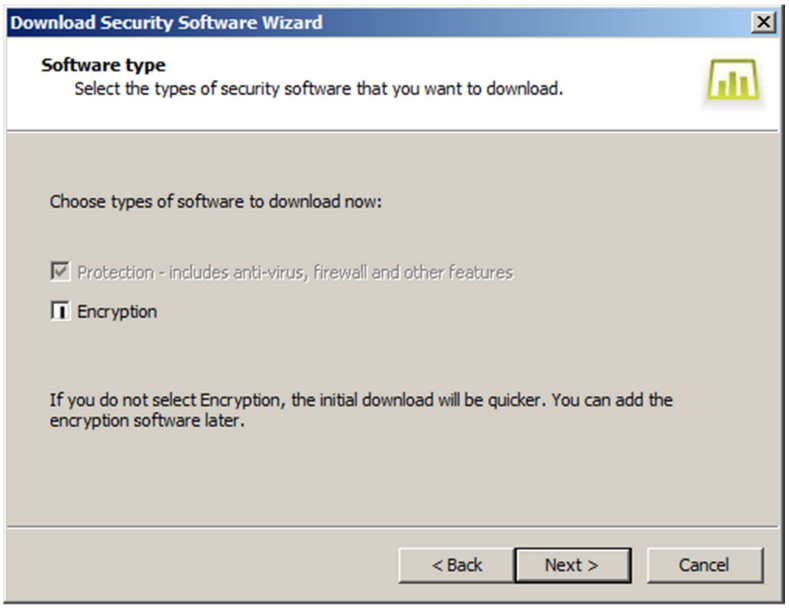



Chọn No và Click Next sau đó chọn các Platforms cần cài đặt: Windows, Linux…

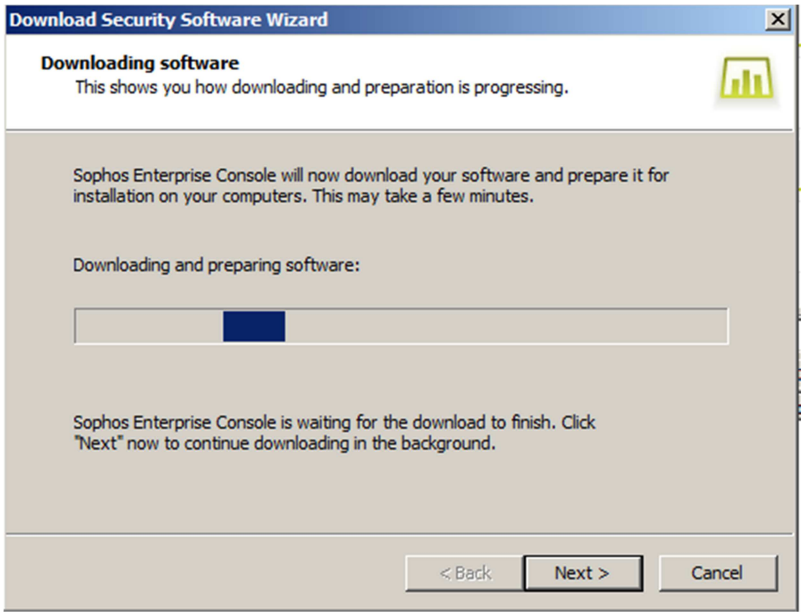


Click Next => Chọn có download phần mềm Encryption hay không.

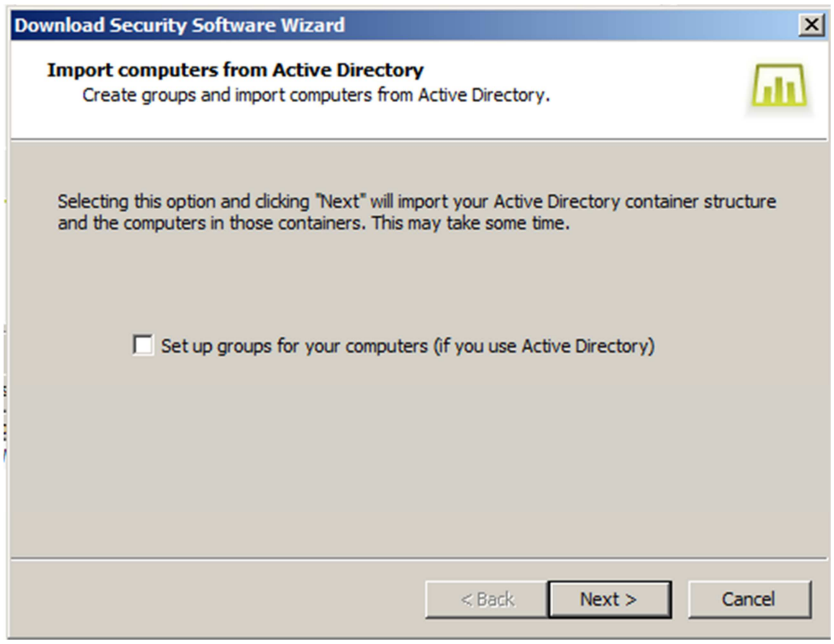
Click chọn Encryption trong trường hợp dùng gói CSS và EDS




Click Next

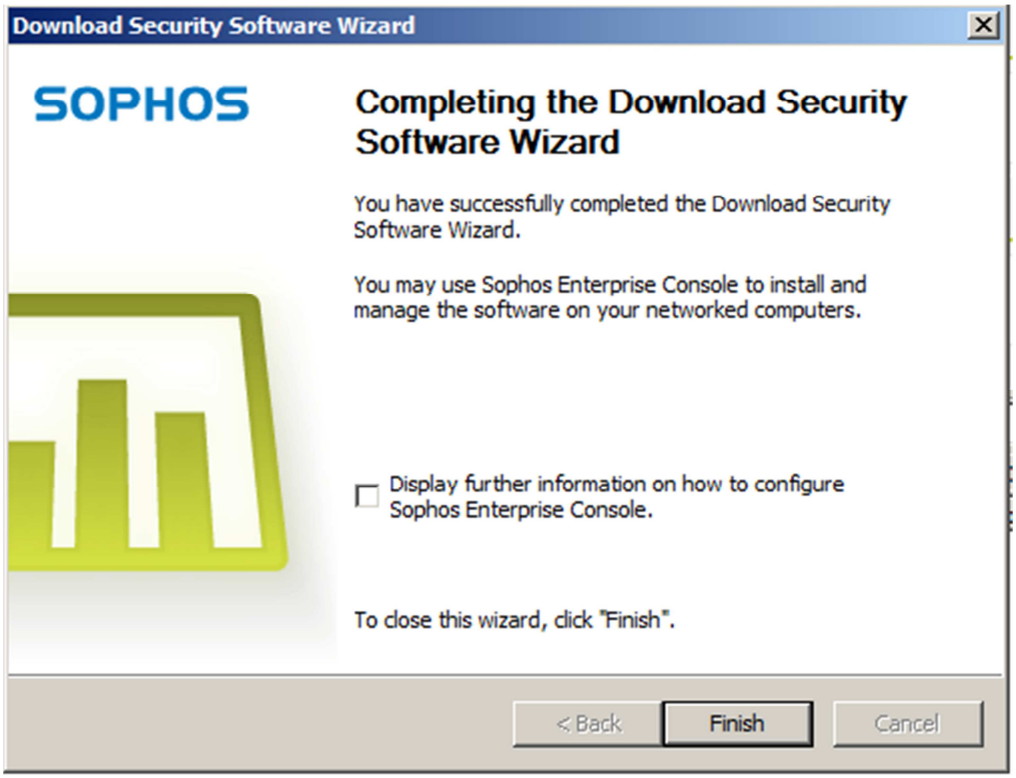



Click Next



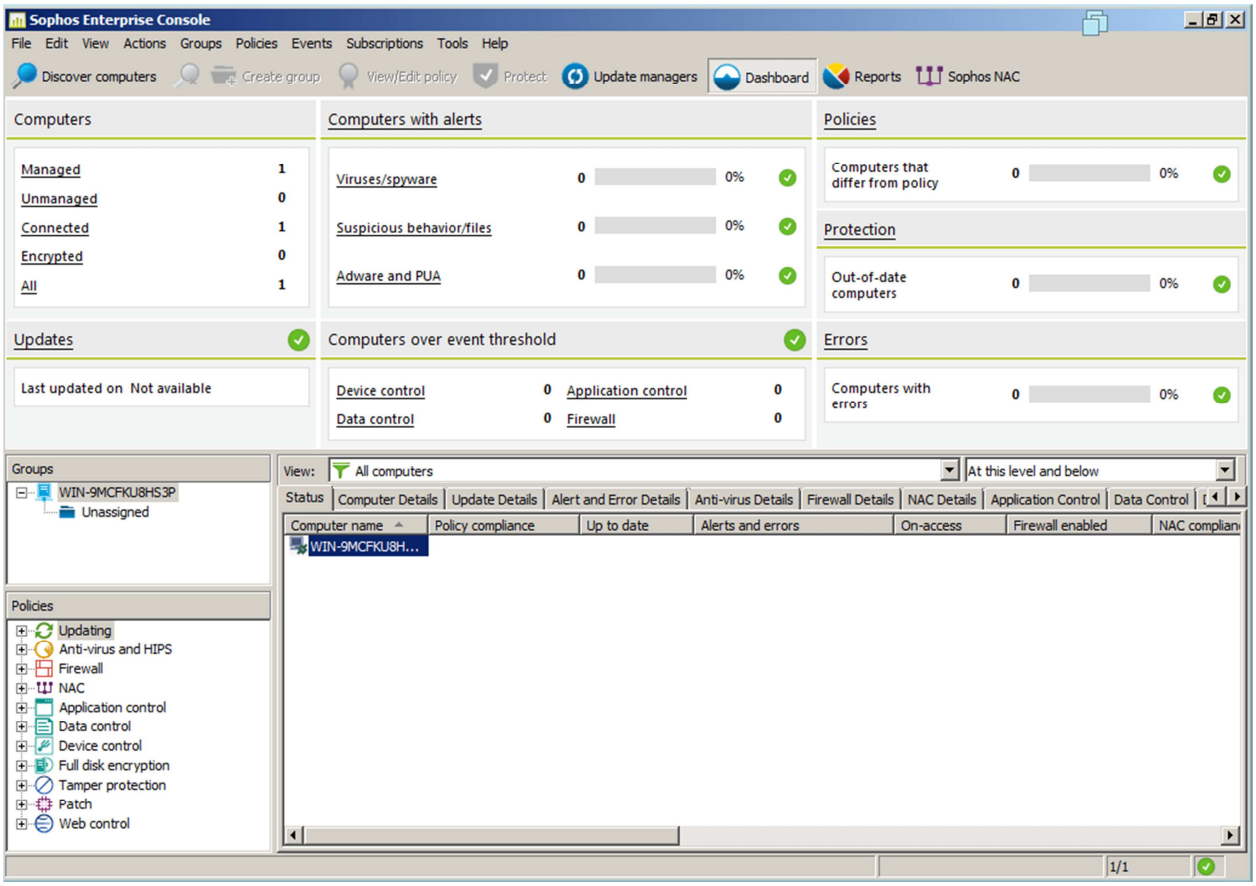

Chọn “Set up groups for your computers” nếu môi trường hệ thống có Active Directory.

Click Next




Click Finish

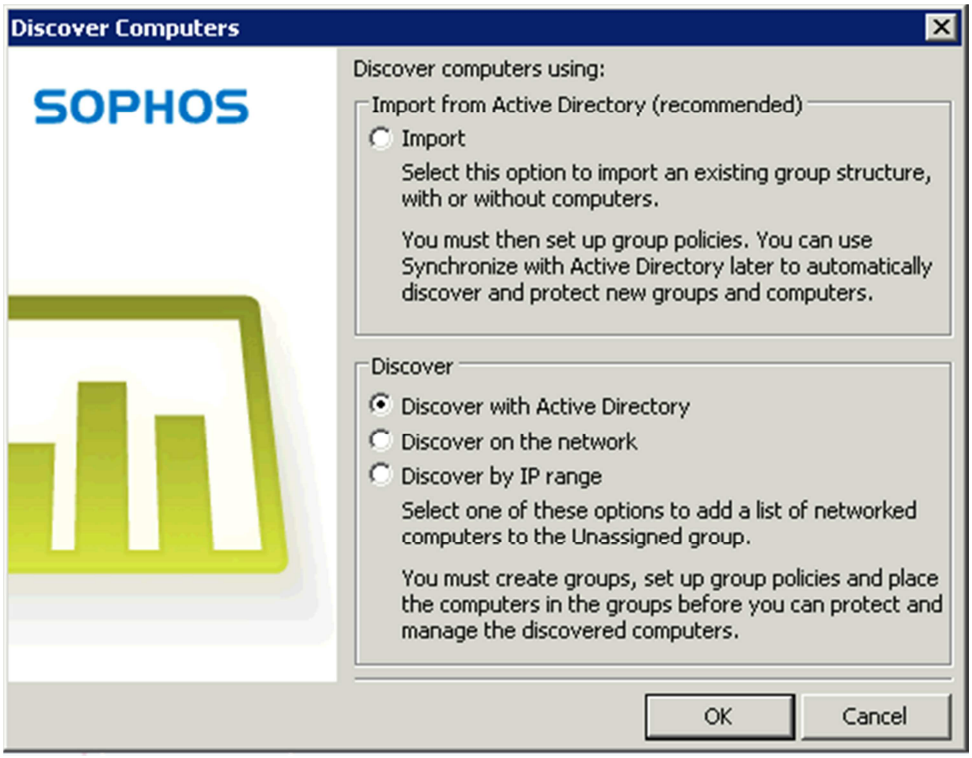
Bảng giao diện Sophos Enterprise Console hiện ra




## 5.2 DISCOVERY COMPUTER

Click nút Discovery Computers ở góc trái phía trên Sophos Enterprise Console

Có 4 lựa chọn để thực hiện phát hiện máy tính trong hệ thống mạng




# 6 BACKUP – RESTORE

Sử dụng công cụ DataBackupRestore.exe đi kèm trong SEC để sao lưu và khôi phục các thông tin sau của SEC:

- Databases.
- Registry settings.
- Account information.
- Configuration files.

Các lưu ý quan trọng

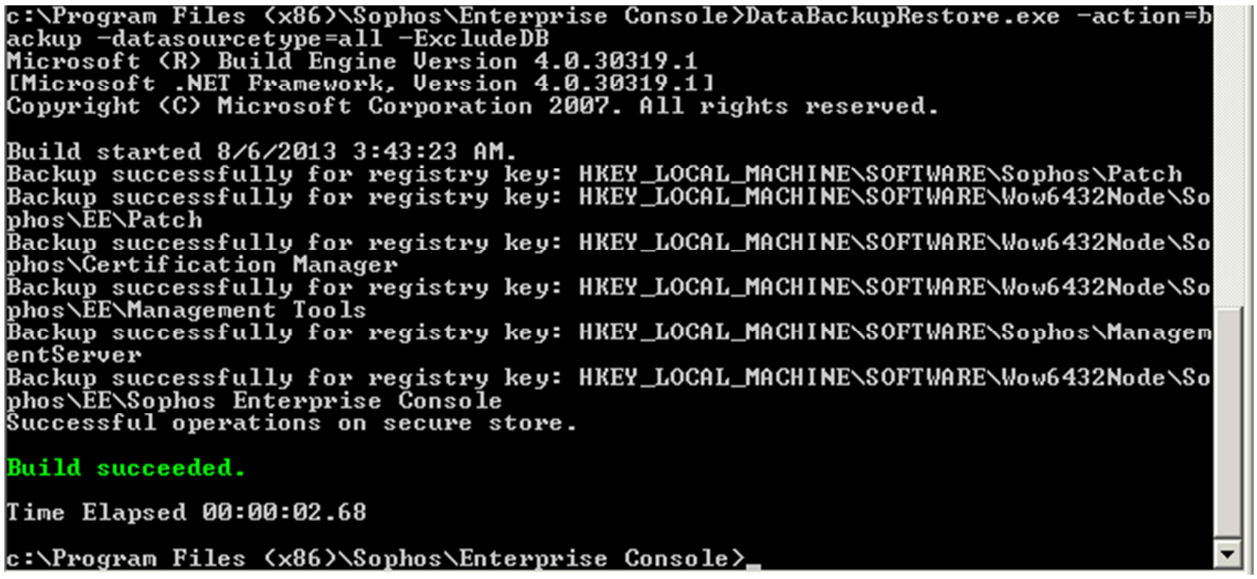
- DataBackupRestore.exe:
  - "C:\Program Files (x86)\Sophos\Enterprise Console\"
  - Sử dụng cmd.exe để chạy chương trình
- Không backup được Database nằm ngoài máy chủ SEC.
- Thư mục chứa file sau khi backup:
  - C:\ProgramData\Sophos\ManagementServer\backup\

Các câu lệnh sử dụng

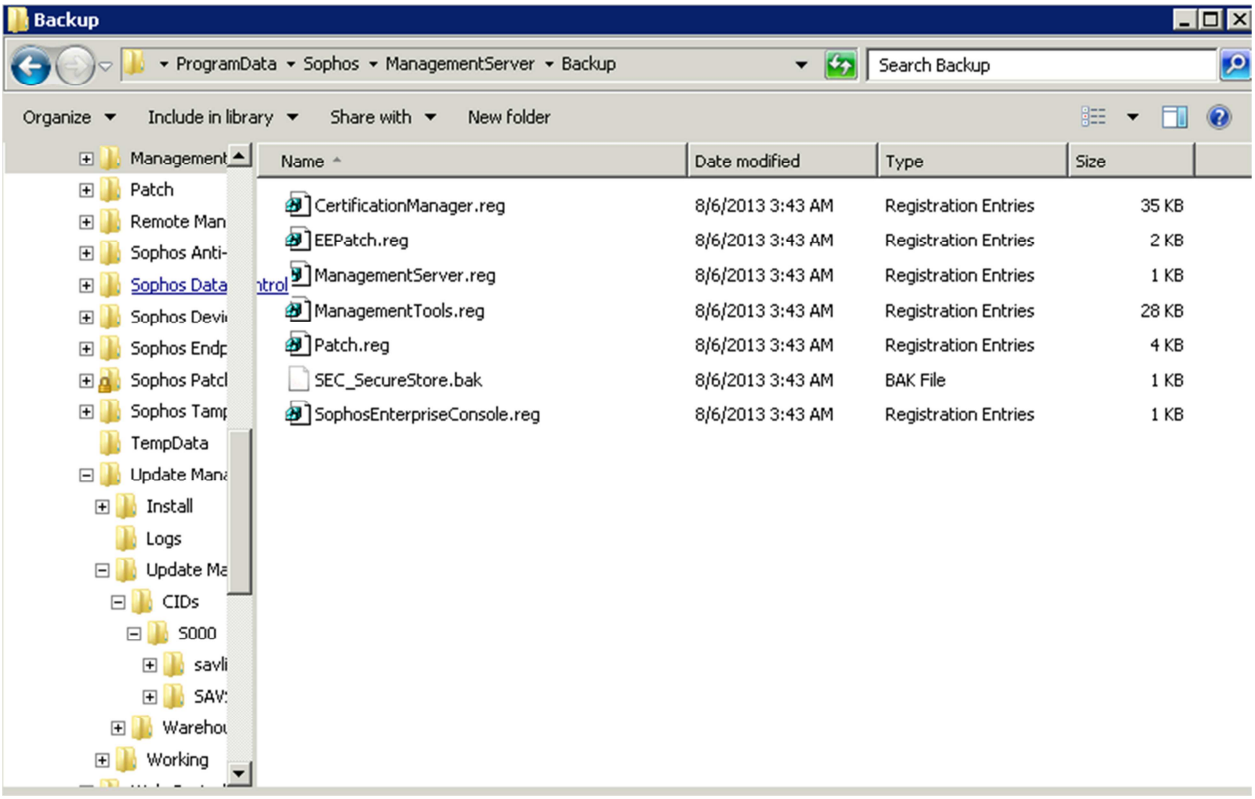
| I want to... | Command |
|---|---|
| backup everything | `DataBackupRestore.exe -action=backup` |

| | |
|---|---|
| restore everything | `DataBackupRestore.exe -action=restore` |
| backup just the database | `DataBackupRestore.exe -action=backup -datasourcetype=database` |
| backup everything but the database | `DataBackupRestore.exe -action=backup -datasourcetype=all -ExcludeDB` |
| restore just the database | `DataBackupRestore.exe -action=restore -datasourcetype=database` |
| restore everything but the database | `DataBackupRestore.exe -action=restore -datasourcetype=all -ExcludeDB` |

Ví dụ Backup exclude Database:




Thư mục chứa backup




Copy và lưu trữ các file trong thư mục backup ở ngoài.

# 7 TẠO GÓI CÀI ĐẶT BẰNG DEPLOYMENTPACKAGE.EXE

Sử dụng file “sdp_121_sfx.exe” (Download ở Sophos Portal hoặc CDROM), extract ra ở đĩa C xong rồi chạy file DeploymentPackage.exe

- **Source Folder**: là folder SophosUpdate, thường như ở đường dẫn trong hình

- **additional setup parameters**:

  -crt R => tự động remove các phần mềm ko tương thích.

  -g “Sophos\PC” => add vào group PC của server Sophos. Anh cần gõ đúng chữ hoa-thường của server và group name. Nếu sai, máy tính cài đặt sẽ nằm trong Unmanaged group.

- **Output package**: thư mục xuất ra file cài đặt

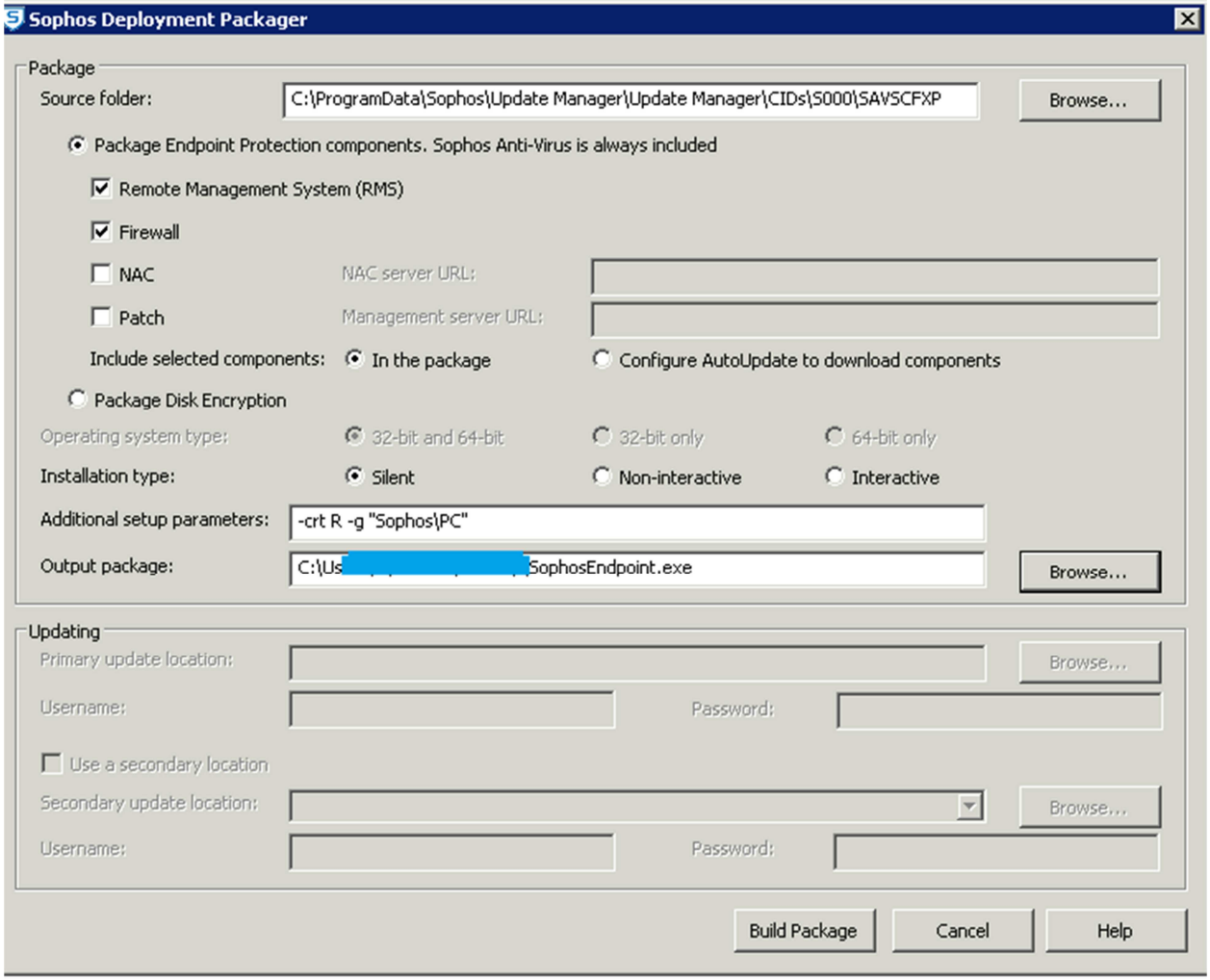
- **Các thông số khác**:

  + chọn tính năng remote management,

  + chọn firewall cho gói cài ở windows 7,8, XP (không chọn cho windows 2008/2012/2003)

  + Chọn cài đặt silent: ko thông báo gì về quá trình cài đặt, click đôi vào file exe, tự chạy.

- Bấm build Package.




Sử dụng DOS command

***DeploymentPackager.exe -cli -mng yes –scf -cidpath "C:\SophosUpdate2\CIDs\S000\SAVSCFXP" -sfxpath "C:\Sophos\Installation Package\1f1y" -crt R -g "Server-Sec\NTSD\Test" -s no -ni no***