



# Sophos Enterprise Console 4.7

**Guia:**

Manual de instalação do Sophos Enterprise Console 4.7

Data do Documento: Julho de 2011



## Conteúdo

Requisitos de Instalação	3
Instalando o Sophos Enterprise Console	4
Configurando as políticas	17
➤ Antivirus e HIPS:	17
➤ Firewall:	20
➤ Application Control:	22
➤ Data Control:	23
➤ Device Control:	24
Importando computadores	25
Definindo regras para determinados grupos	27
Instalando remotamente	28

## Requisitos de Instalação

- Requisitos para instalar o Sophos Enterprise Console:

<http://www.sophos.com/en-us/products/endpoint/endpoint-security-and-data-protection/components/management-console/system-requirements.aspx>

- Requisitos para instalar o Sophos Antivírus:

Windows: <http://www.sophos.com/en-us/products/endpoint/endpoint-security-and-data-protection/components/anti-virus-protection/windows/system-requirements.aspx>

Linux: <http://www.sophos.com/en-us/products/endpoint/endpoint-security-and-data-protection/components/anti-virus-protection/linux/system-requirements.aspx>

Mac OS X: <http://www.sophos.com/en-us/products/endpoint/endpoint-security-and-data-protection/components/anti-virus-protection/mac/system-requirements.aspx>

NetApp: <http://www.sophos.com/en-us/products/endpoint/endpoint-security-and-data-protection/components/anti-virus-protection/netapp/system-requirements.aspx>

UNIX: <http://www.sophos.com/en-us/products/endpoint/endpoint-security-and-data-protection/components/anti-virus-protection/unix/system-requirements.aspx>

- Requisitos para instalação remota (usando o Sophos Enterprise Console para instalar o Sophos Antivírus em uma estação):

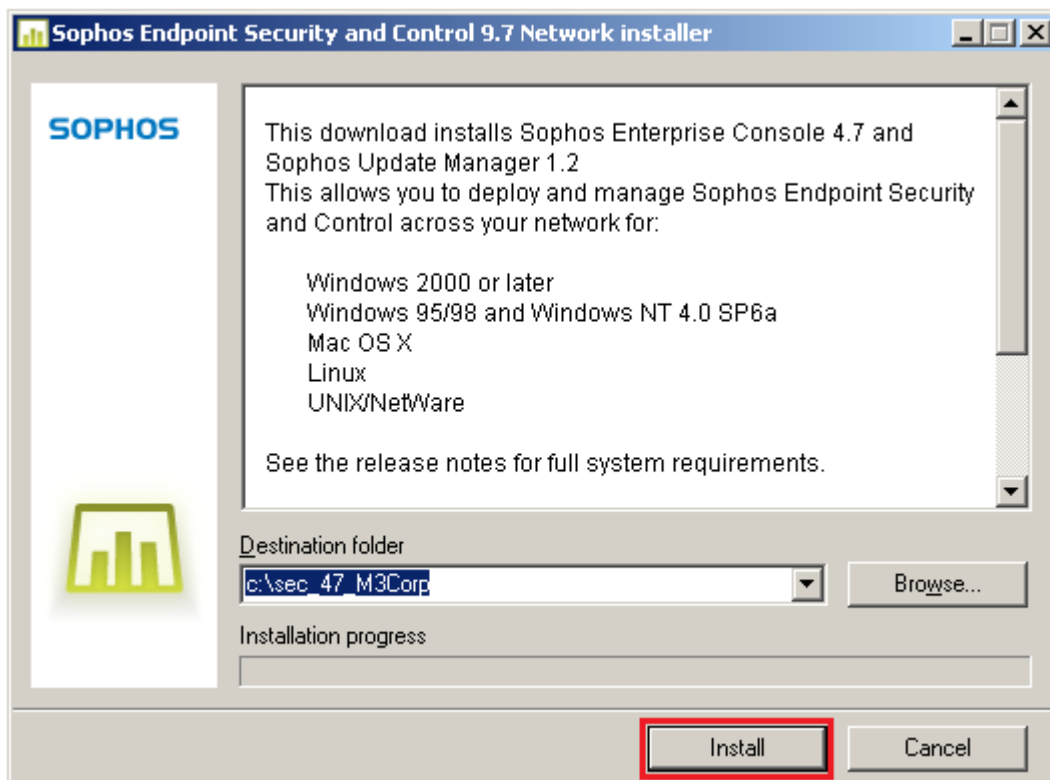
[http://www.sophos.com/sophos/docs/eng/instguid/sesc\\_97\\_asgeng.pdf](http://www.sophos.com/sophos/docs/eng/instguid/sesc_97_asgeng.pdf) (página 46 até 48, item 11.1.3 - Prepare for installation of anti-virus software)

## Instalando o Sophos Enterprise Console

1- Execute o instalador [sec\\_47\\_sfx.exe](#) (Clique para baixar).



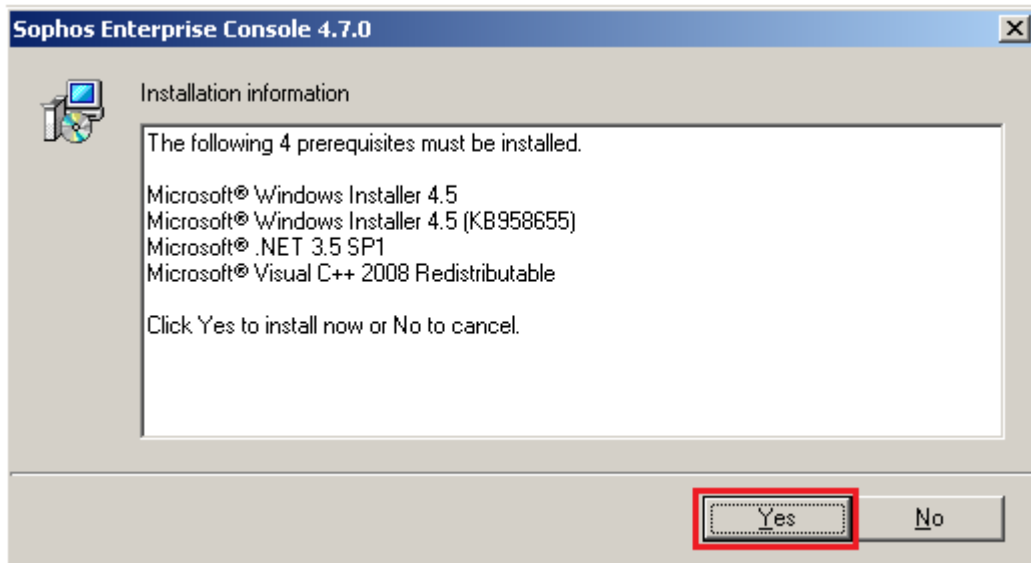
2- Clique em **Install**



### 3- Pré requisitos:

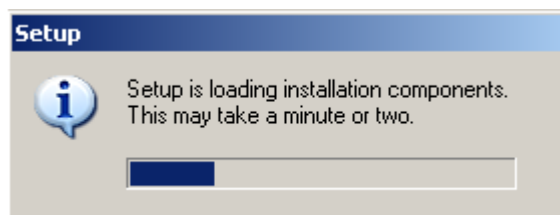
Será solicitado o ServicePack 2 do Windows 2003, caso a instalação seja no Windows 2003

Alem deste será solicitado quatro Pré requisitos constados abaixo, caso não tenha nenhum deles instalado



Instale os pré requisitos.

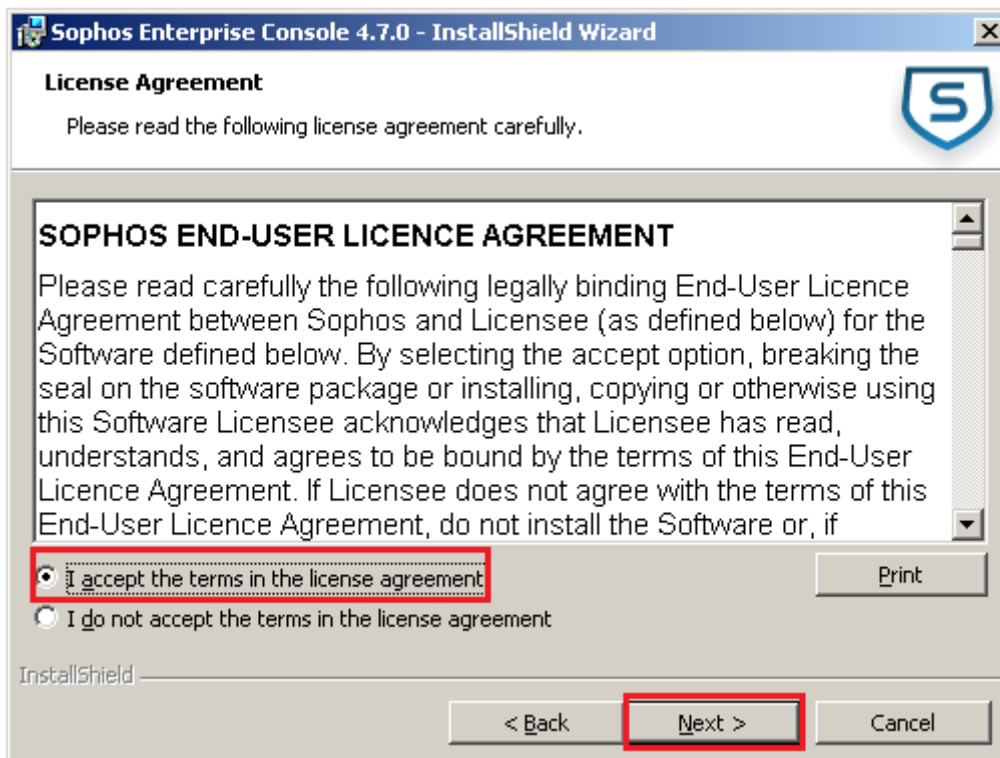
Obs: O Sophos instala os pré-requisitos não é necessário baixá-los



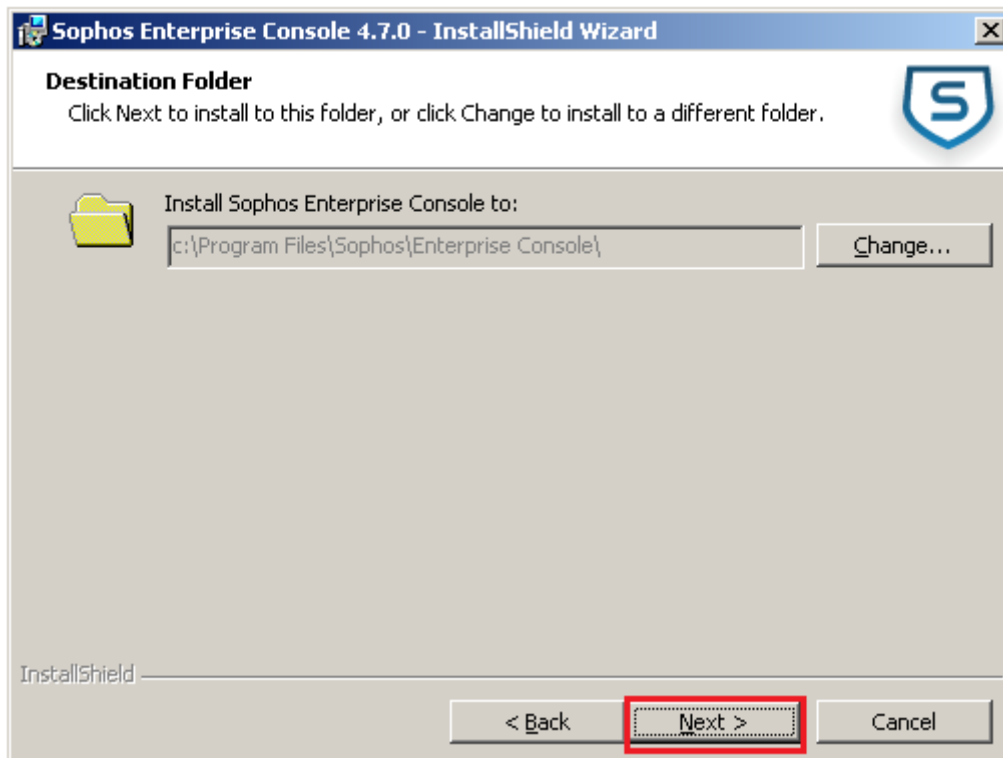
4- Clique em **Next**



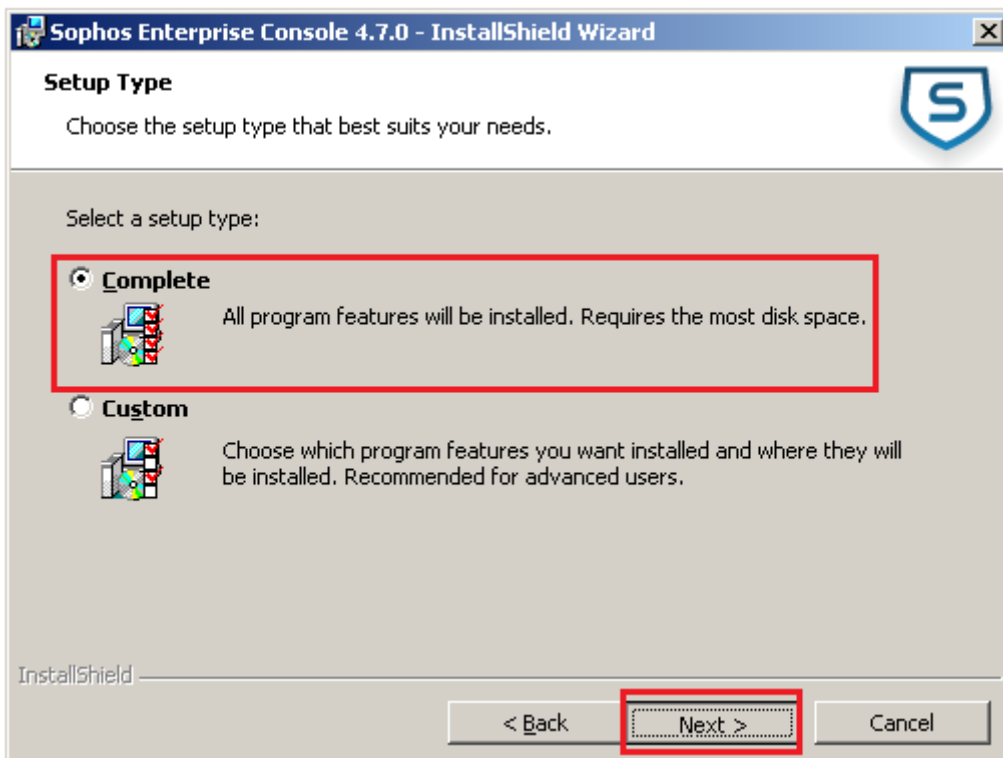
5- Clique em **"I accept the terms in the license agreement"** e clique em **Next**.



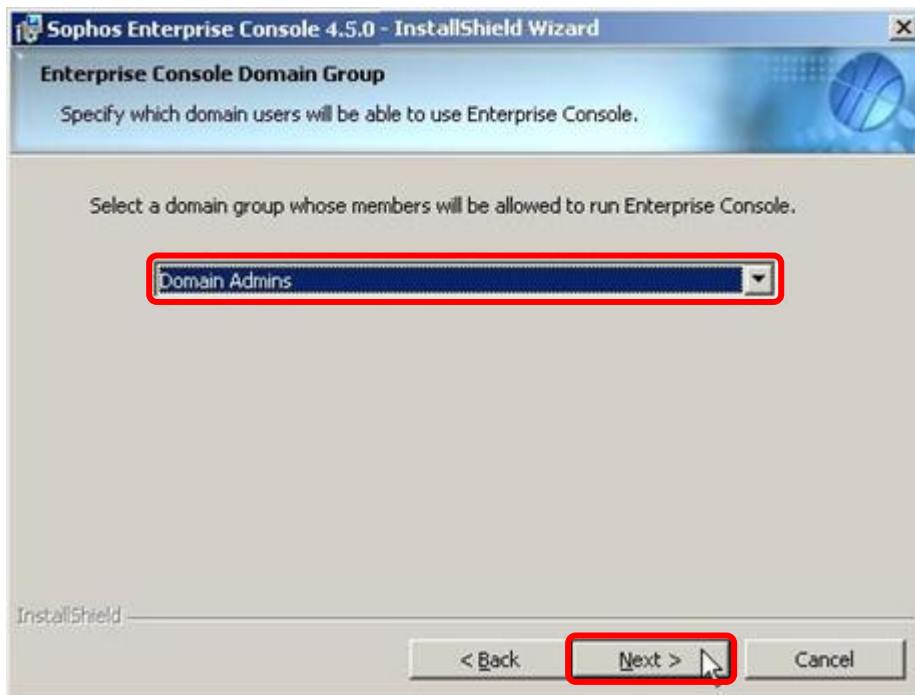
6- Caso queira modificar o destino da instalação, clique em **Change**, após clique em **Next**.



7- Clique em **Next** para instalar o **Sophos Enterprise Console 4.7** com todos componentes.

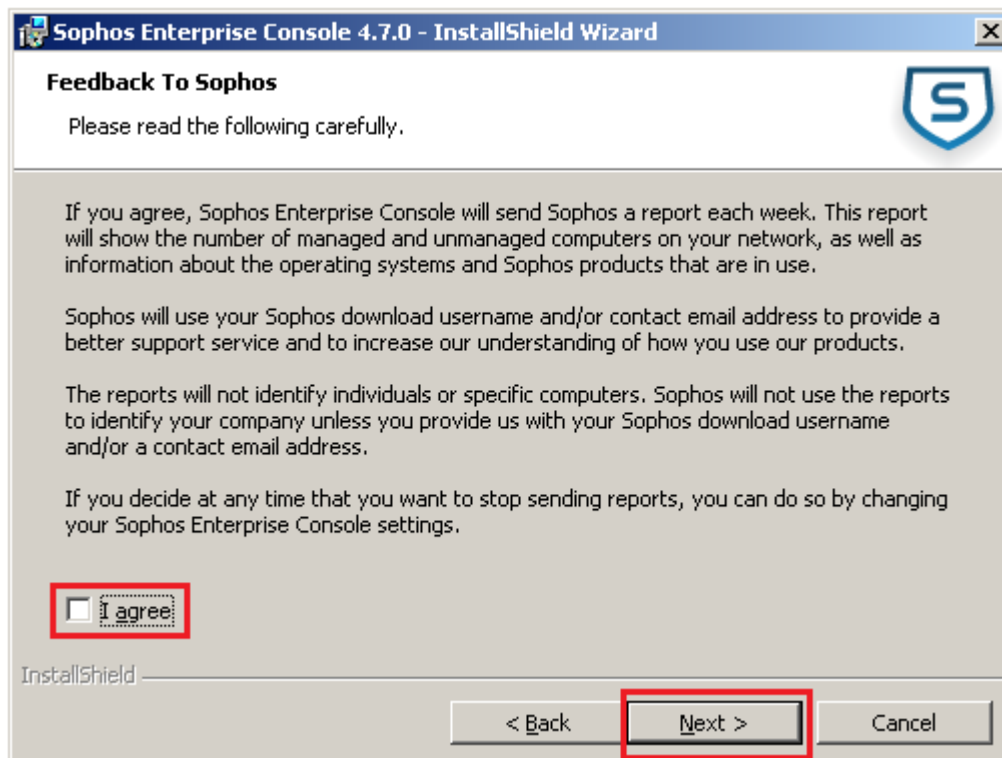


8- Selecione o grupo de usuários que poderão gerenciar a Enterprise Console, clique em **Next**:



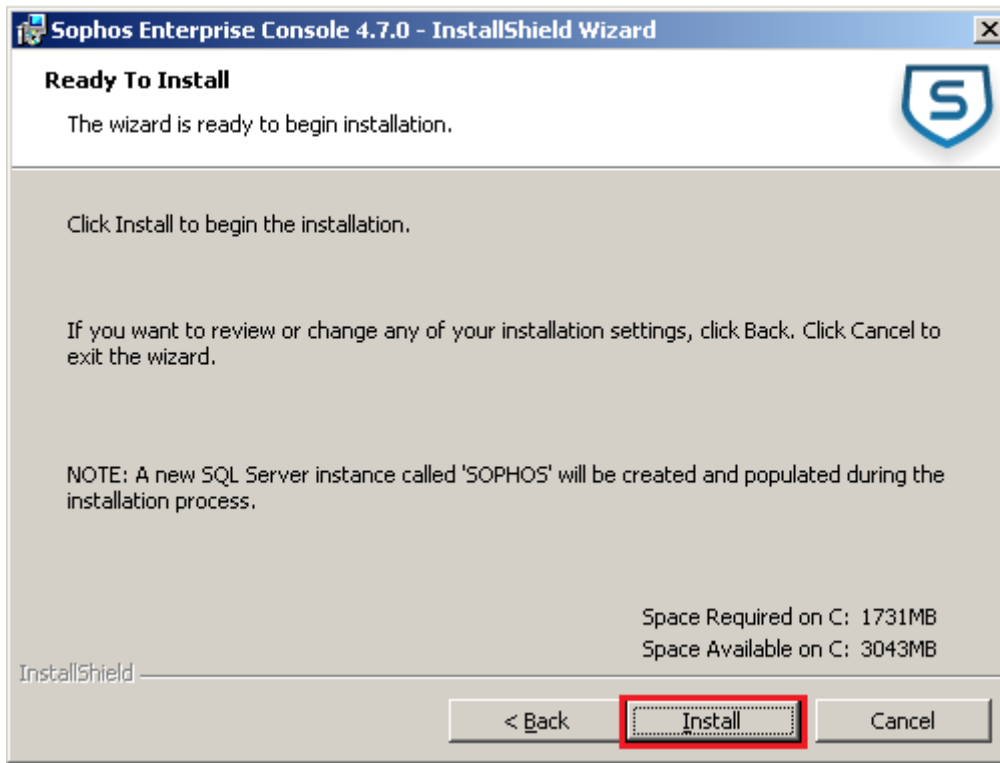
OBS: Caso a máquina em que você está instalando o Sophos Enterprise Console não estiver ingressado em um domínio, esta tela não irá aparecer, pule para o passo 9.

9- Retire o **I agree** e após clique em **Next** para continuar a instalação:

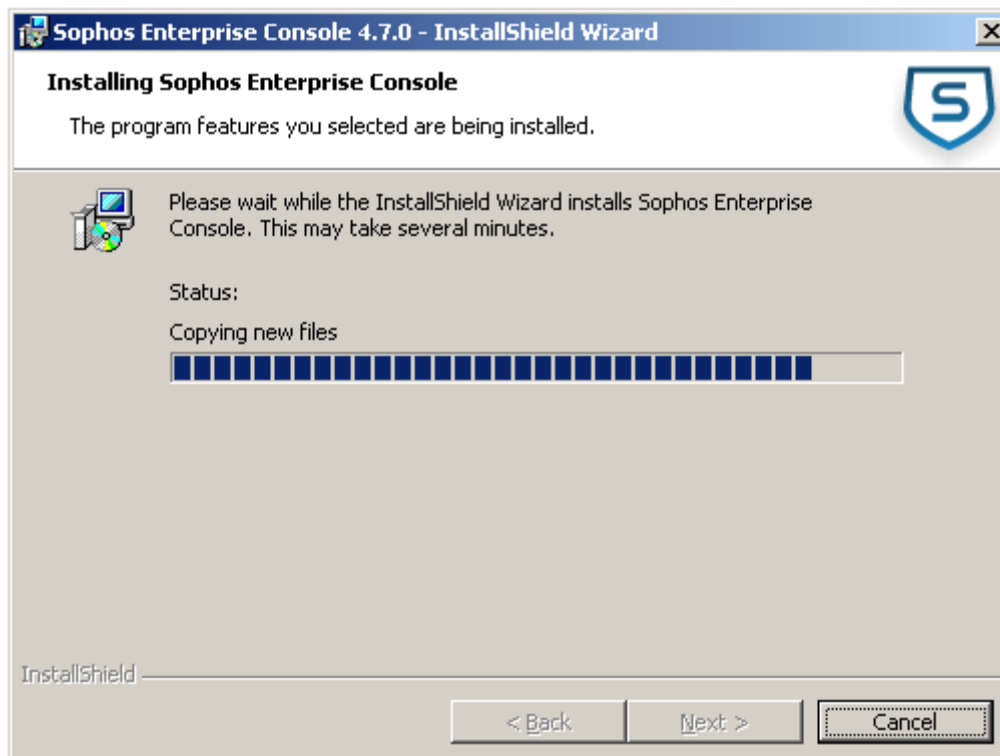




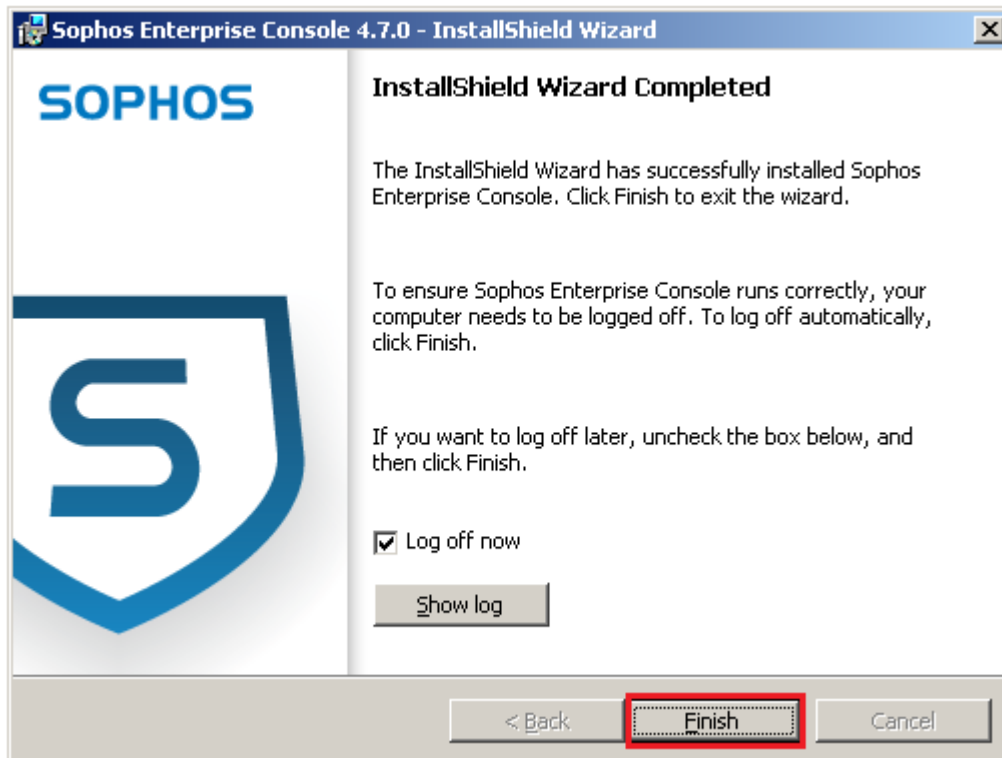
10- Clique em **Install** para iniciar a instalação



11- Aguarde a instalação concluir



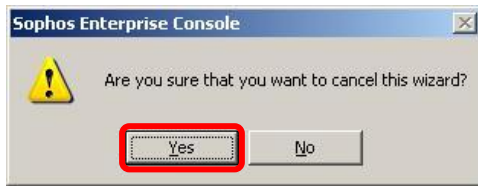
12- Após concluir a instalação, será necessário fazer **log off**:



13- Após fazer login, irá abrir o Wizard, clique em **Cancelar**:



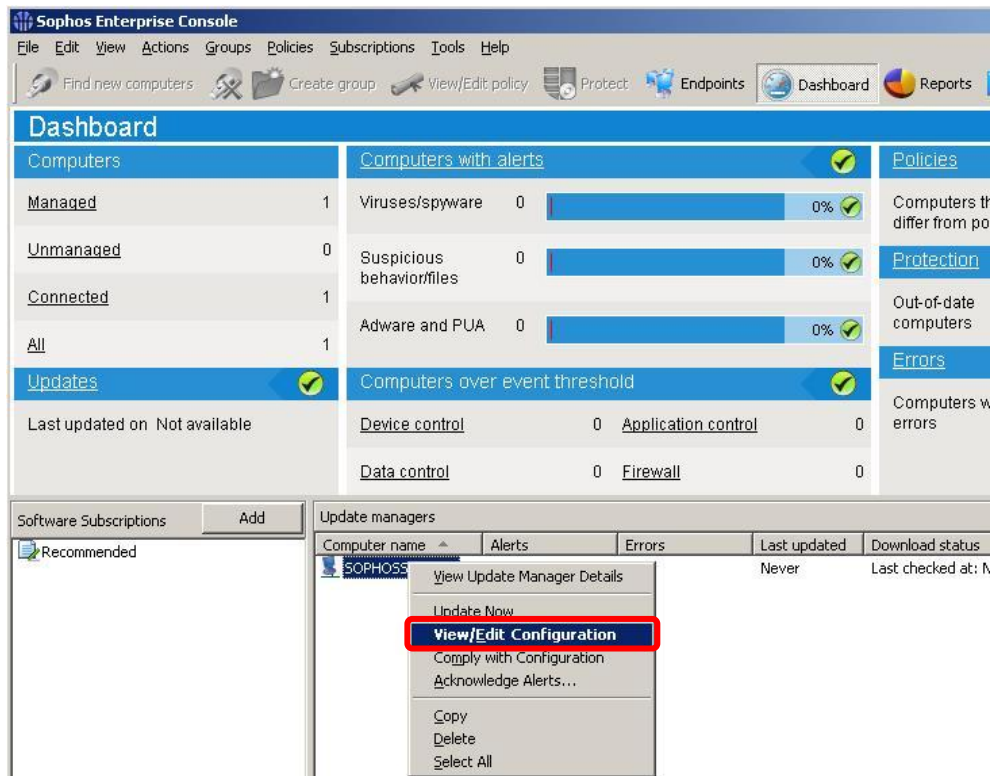
#### 14- Clique em Yes



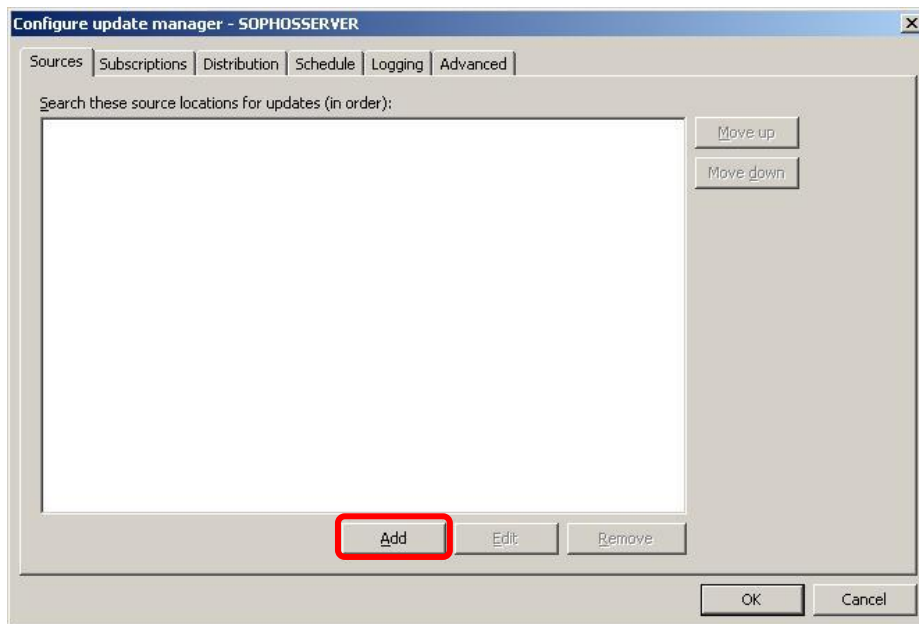
#### 15- Clique em Update Managers



#### 16- Clique com o botão direito em View/Edit Configuration



### 17- Clique em **Add**

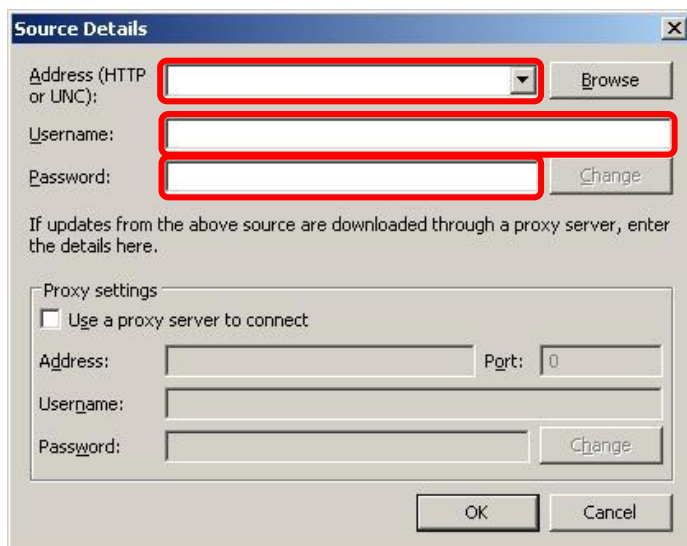


### 18- Preencha com os dados enviados do Trial ou Ativação

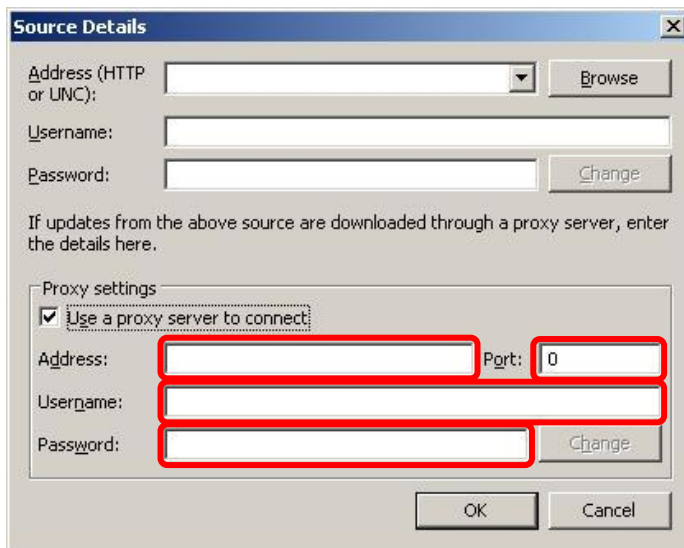
Trial: Address = Sophos

Ativação: Address = <http://sophosv97-srv01.m3corp.com.br>

Obs: Caso esteja testando a solução utilize a o Address Trial, caso for Cliente utilize o Address ativação



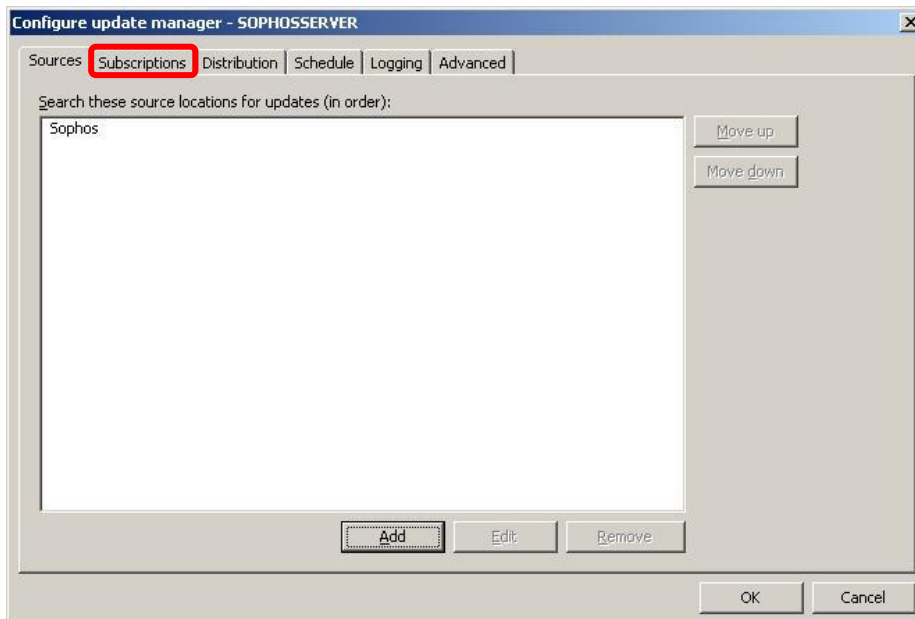
19- Caso use Proxy em sua rede, preencha os dados, após clique em **OK**



The dialog box is titled "Source Details" and contains the following fields and controls:

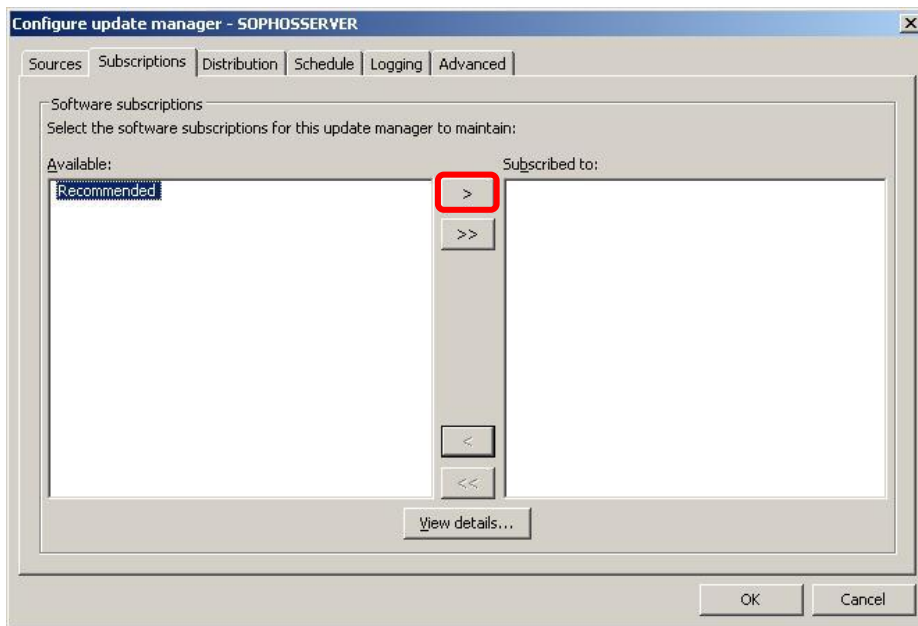
- Address (HTTP or UNC): A text box with a dropdown arrow and a "Browse" button.
- Username: A text box.
- Password: A text box with a "Change" button.
- Proxy settings section:
  - Use a proxy server to connect:
  - Address: A text box with a red border.
  - Port: A text box containing "0" with a red border.
  - Username: A text box with a red border.
  - Password: A text box with a red border and a "Change" button.
- OK and Cancel buttons at the bottom.

20- Clique em **Subscriptions**

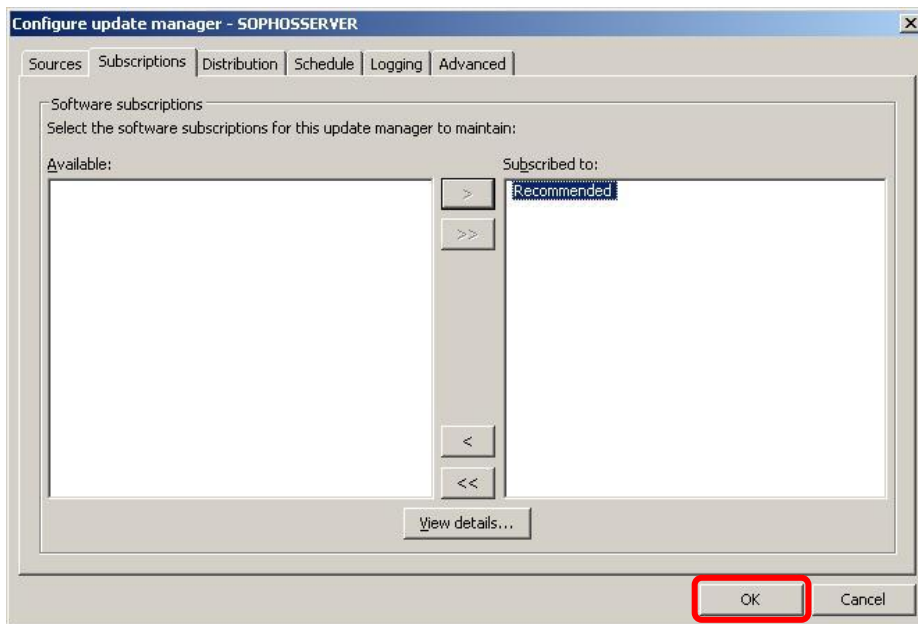


The dialog box is titled "Configure update manager - SOPHOSSERVER" and has several tabs: Sources, **Subscriptions**, Distribution, Schedule, Logging, and Advanced. The "Subscriptions" tab is selected and highlighted with a red box. The main area contains a list of source locations for updates, with "Sophos" listed. To the right of the list are "Move up" and "Move down" buttons. At the bottom of the list area are "Add", "Edit", and "Remove" buttons. At the bottom of the dialog are "OK" and "Cancel" buttons.

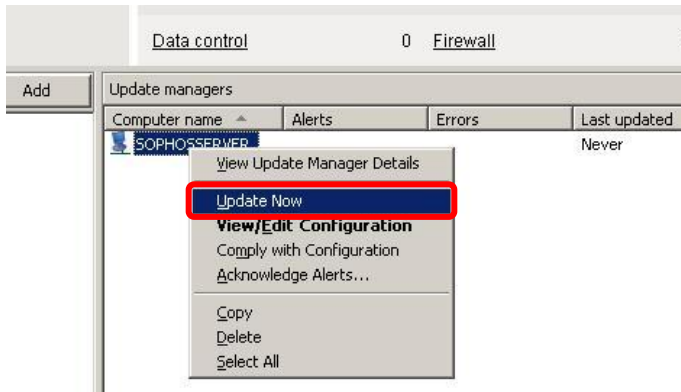
21- Seleccione **Recommended** e mova-o para a direita



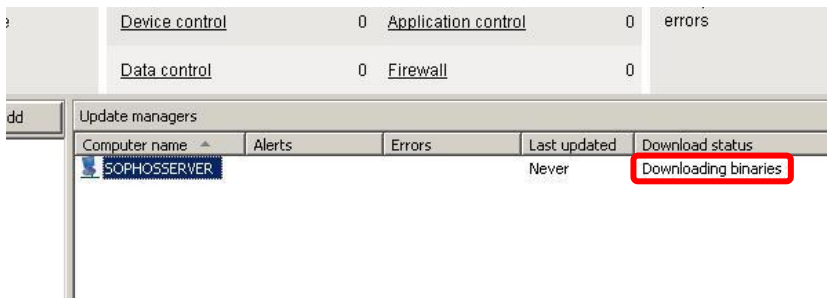
22- Clique em **OK**



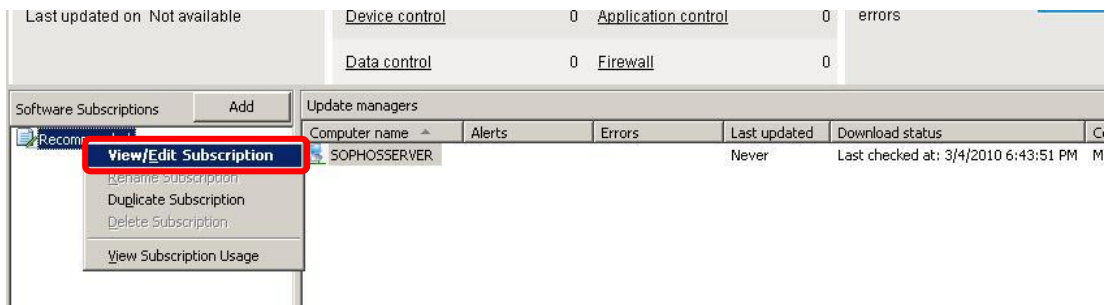
23- Clique com o direito no servidor e em **Update Now**



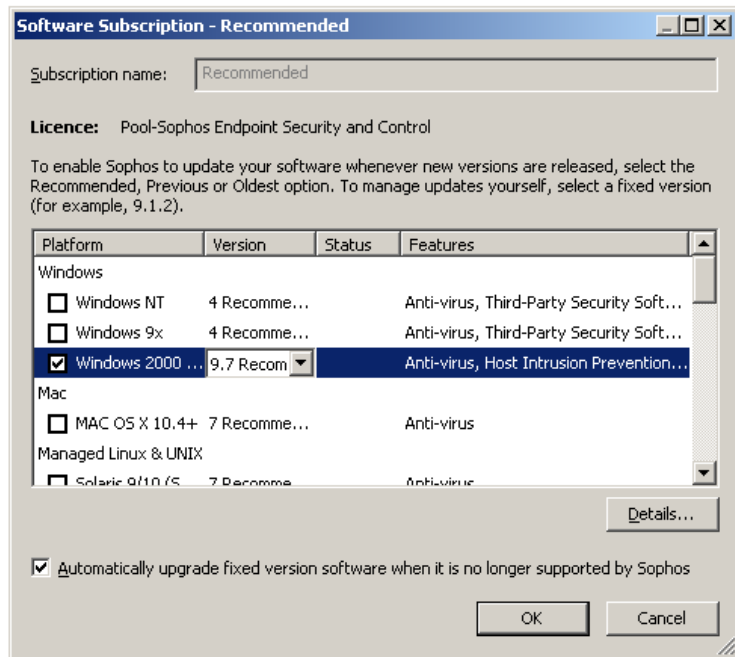
24- Aguarde o fim do **Downloading binaries**, esta etapa pode demorar alguns minutos



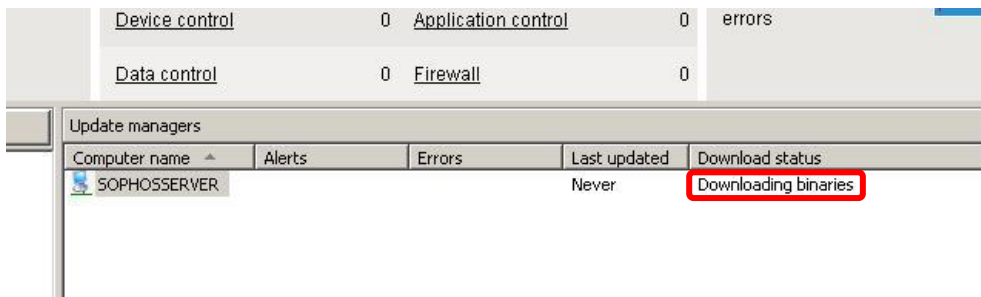
25- Ao fim do download, clique com o direito em **Recommended** e em **View/Edit Subscription**



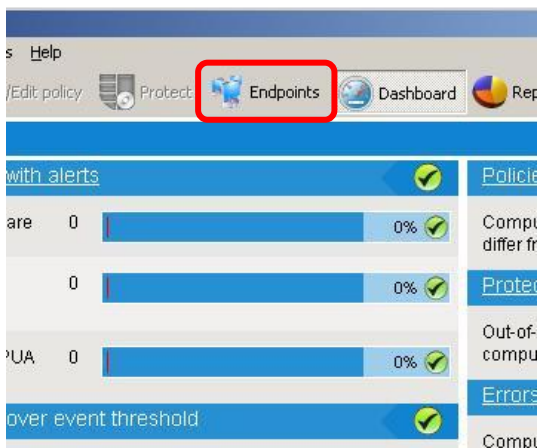
26- Selecione **Windows 2000 and Above** para Windows 2000 ou superiores (XP, Vista, 7, etc)



27- Aguarde o final do Download dos binários

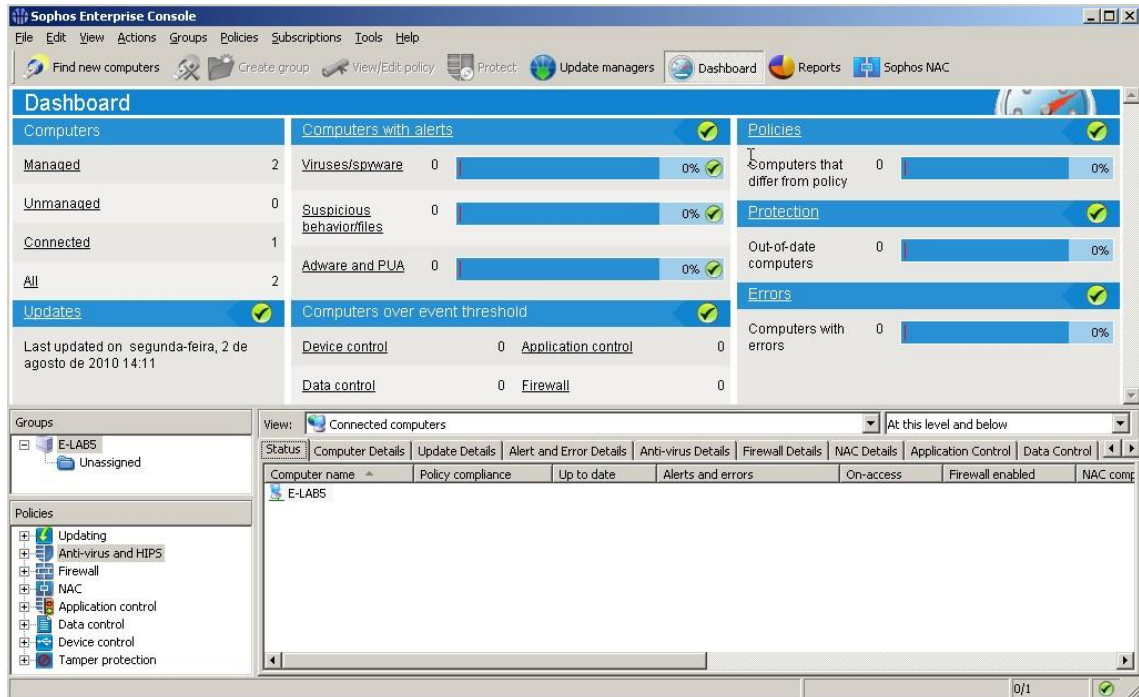


28- Ao fim do download, clique em **Endpoints** para iniciar a proteção das máquinas





## 29 - Tela inicial da Enterprise Console



## Configurando as políticas

Abaixo veja as configurações recomendadas:

### ➤ Antivirus e HIPS:

OBS: HIPS é a tecnologia que irá proteger sua rede de ameaças desconhecidas e com comportamento suspeito, mais informações sobre o HIPS:

<http://www.sophos.com/support/knowledgebase/article/25044.html>

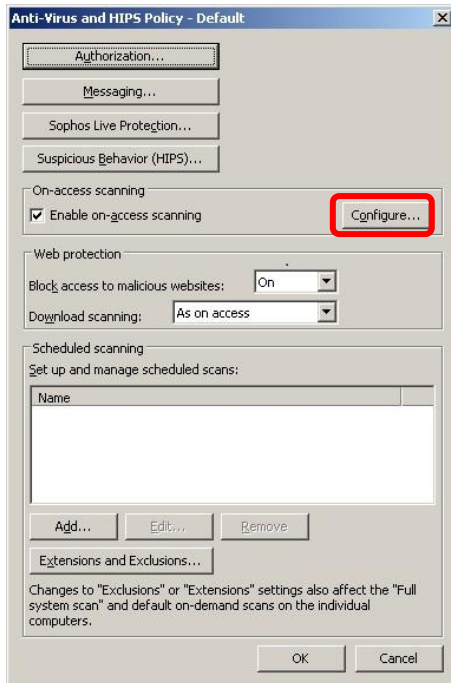
1- Abra o Sophos Enterprise Console

2- No quadro **Policies** (localizado no canto esquerdo inferior) expanda **Anti-vírus and HIPS**:

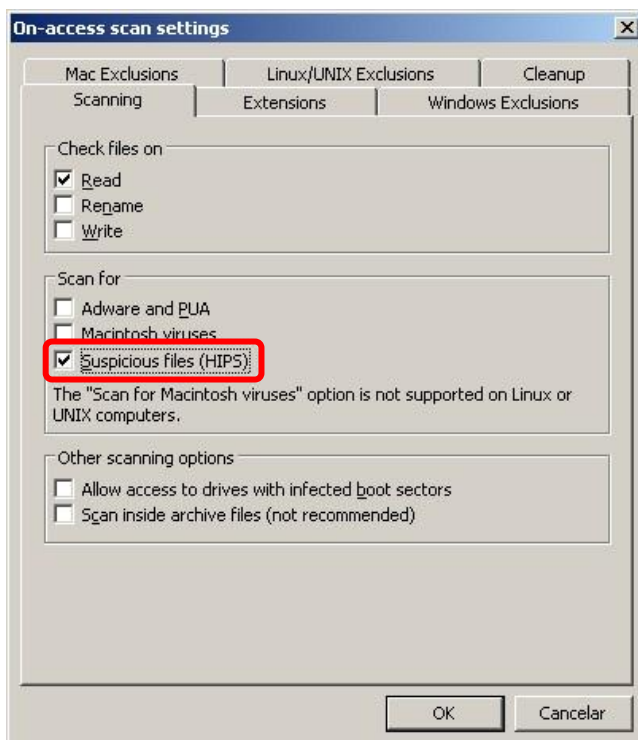


3- Clique duas vezes na política de Antivírus e HIPS a ser editada (ou clique com o botão direito e clique em **View/Edit Policy**)

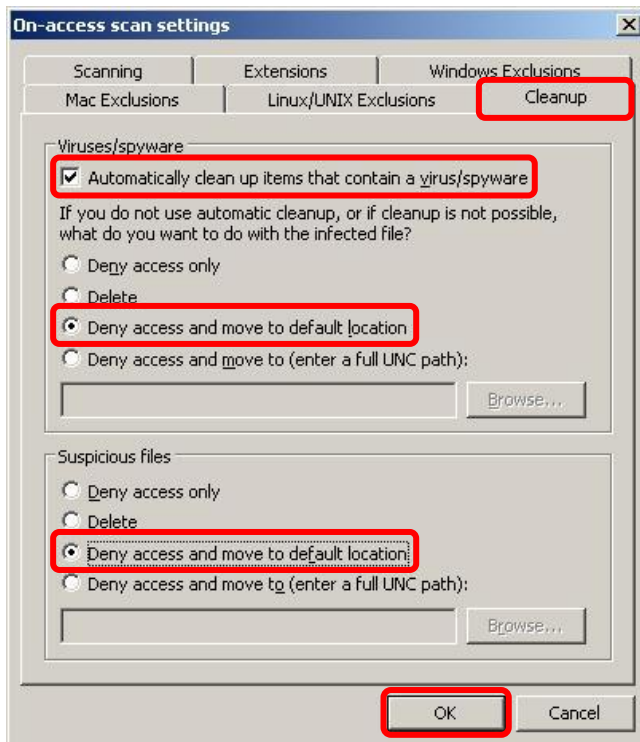
4- Clique em **Configure...**, após abrir a política de **Antivírus and HIPS**:



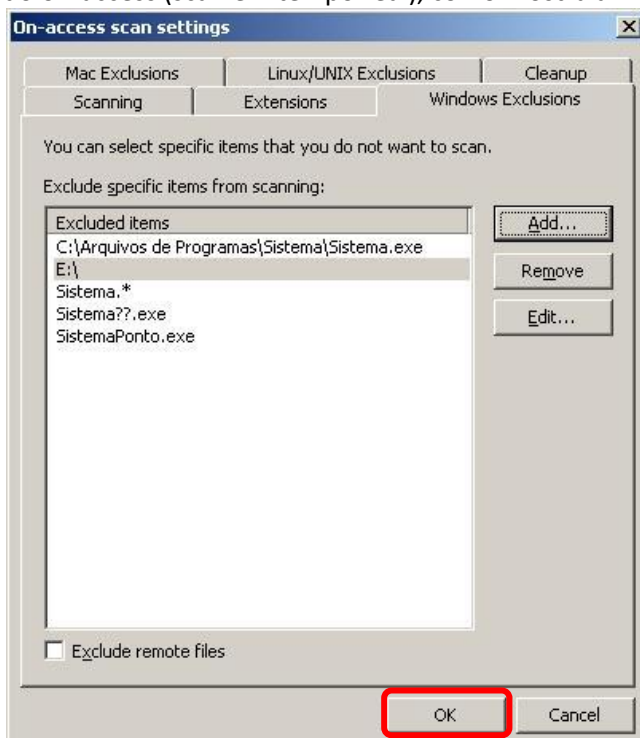
5- Marque **Suspicious files (HIPS)** na aba **Scan for** para habilitar a análise pelo HIPS



6- Clique na guia **Cleanup**, e marque a Box **Automatically clean up item that contain a vírus/spyware**, e selecione as ações que deveram ser tomadas caso a limpeza falhe ou caso a box não esteja marcada.



7- As guias **Windows Exclusions**, **Linux/UNIX Exclusions** e **Mac Exclusions** são para adicionar nomes de arquivos, pastas, arquivos com um determinado caminho e unidades para a exclusão do on-access (scan em tempo real), como mostra a imagem abaixo:



OBS: marcando a opção **Exclude remote files** os arquivos remotos (via compartilhamento de arquivos) não serão verificados, não marcando esta opção, o computador do usuário que esta acessando um compartilhamento irá verificar os arquivos compartilhados da máquina remota.

## ➤ Firewall:

OBS: existem 3 métodos para configurar o firewall:

A. Criando todas as regras pela console (baseando em porta local e remotas, IP local e remoto)

B. Instalando o Sophos Client Firewall em uma máquina, acionar o modo interativo (permitindo ao usuário a decidir se permite ou não as conexões) e após terminar a configuração, apenas importando as configurações para a console, aplicando em todas outras máquinas. (Recomendado)

C. Instalando o Sophos Client Firewall em algumas máquinas, usando estas máquinas para gerar eventos na console e pela console criar as políticas para cada evento. (Recomendado)

Vamos utilizar o **método C** (instalando o firewall em uma máquina para gerar eventos na console):

1- No endpoint (máquina que possui o firewall) abra o IE (Internet Explorer)

2- Tente acessar um site.

OBS: A política padrão do firewall é bloquear, sendo necessário permitir ou não os eventos, podendo mudar a política para liberar tudo e bloqueando os eventos reportados, sendo também possível mudar a política padrão para monitorar o tráfego não bloqueando nada, vamos deixar a política para bloquear tudo e liberando os eventos permitidos.

3- Após a tentativa de acessar o site, será enviado o evento para o Sophos Enterprise Console, abra o Sophos Enterprise Console e clique 2 vezes na máquina que gerou o evento (ou clique com o botão direito e clique em **View computer details**)

### Latest firewall events

Date/time	Event type	File name	File version
9/10/2009 09:56:15	New application	ieexplore.exe	7.00.6000.16735 (vista_gdr.080820-1506)
9/10/2009 09:55:24	No application rule	svchost.exe	5.1.2600.5512 (xpsp.080413-2111)
9/10/2009 09:55:24	No application rule	svchost.exe	5.1.2600.5512 (xpsp.080413-2111)
9/10/2009 09:54:28	No application rule	svchost.exe	5.1.2600.5512 (xpsp.080413-2111)

Como podemos ver, um novo aplicativo foi reportado, feche a janela.

4- Abra a política de firewall

5- Clique em **Advanced firewall policy**

6- Clique em **Configure**

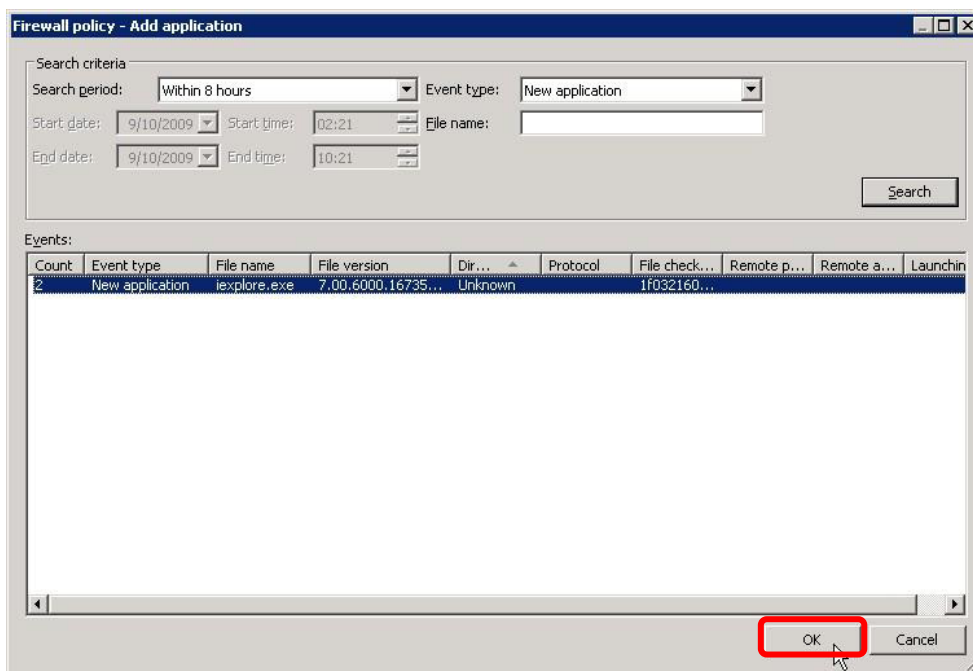
Note que na janela que abriu a opção “Use checksums to authenticate application” esta habilitada, caso queira usar a autenticação por checksum para permitir que o aplicativo navegue, será necessário adicionar o checksum de cada versão do aplicativo usado na guia “Checksum”

7- Clique na guia **Applications**

8- Clique em **Add**

9- Faça a pesquisa do evento, mudando campo **Event type** para **New application**, clique em **Search**

10- Selecione o evento e clique em **OK**



11- Clique em **OK** para aplicar a política.

➤ **Application Control:**

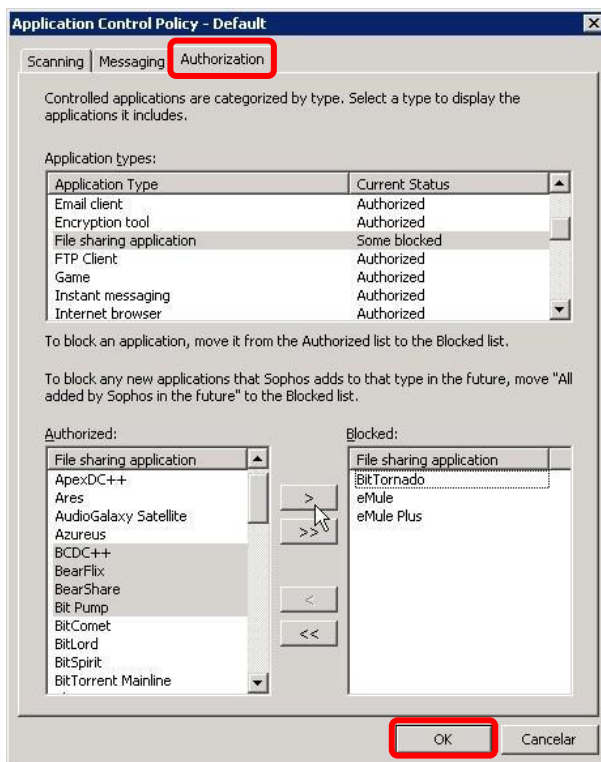
Com o Application control você pode controlar aplicativos como programas P2P, games, IM, etc.

1- Abra a política de Application control

2- Selecione a Box **Enable on-access scanning** para habilitar o controle de aplicativos

3- Clique na aba **Authorization**

4- Selecione a categoria e então adicione o aplicativo a ser bloqueado, como mostra na imagem abaixo:



➤ **Data Control:**

Com o Data Control você pode controlar arquivos e conteúdos que estão saindo da máquina, por exemplo: arquivos que contem as palavras “informação secreta” não poderão ser transferidos, ou permitir mas gerar evento na console

1- Abra a política de Data control

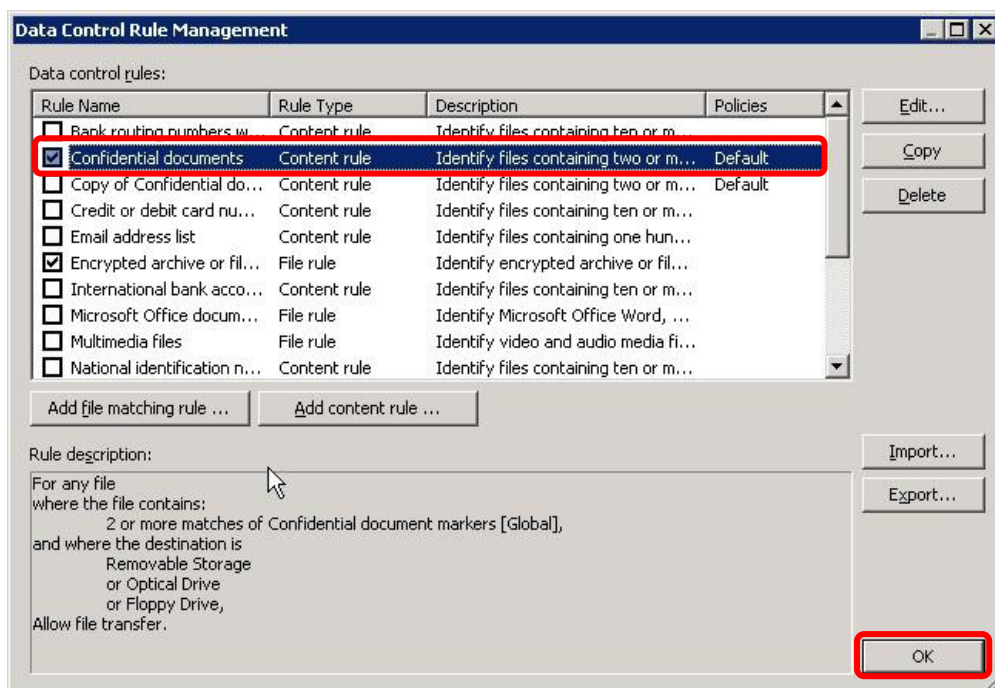
2- Marque a Box **Enable data control scanning** para habilitar este controle

3- Clique em **Manage Rules** para criar as regras

4- Nesta janela já existe uma serie de modelos, podendo criar novas regras, editar as regras existentes e assim como criar copias das regras existentes e editá-las.

5- Clique em Add file matching rule para criar uma regra para arquivos e Add content rule para adicionar uma regra para um determinado conteúdo

6- Para habilitar a política, selecione a Box:



➤ **Device Control:**

**Importante:** O controle de dispositivo da Sophos não deverá ser implementado juntamente com controle de dispositivo de software de outros fabricantes.

O controle de dispositivos permite que você previna usuários de usar dispositivos de hardware externos não autorizados, mídias de armazenamento removíveis e tecnologias de redes sem fio (wireless) em seus computadores. Isso pode ajudar a reduzir significativamente sua exposição à perda de dados acidentais e restringir a habilidade dos usuários de introduzir softwares do ambiente externo à sua rede.

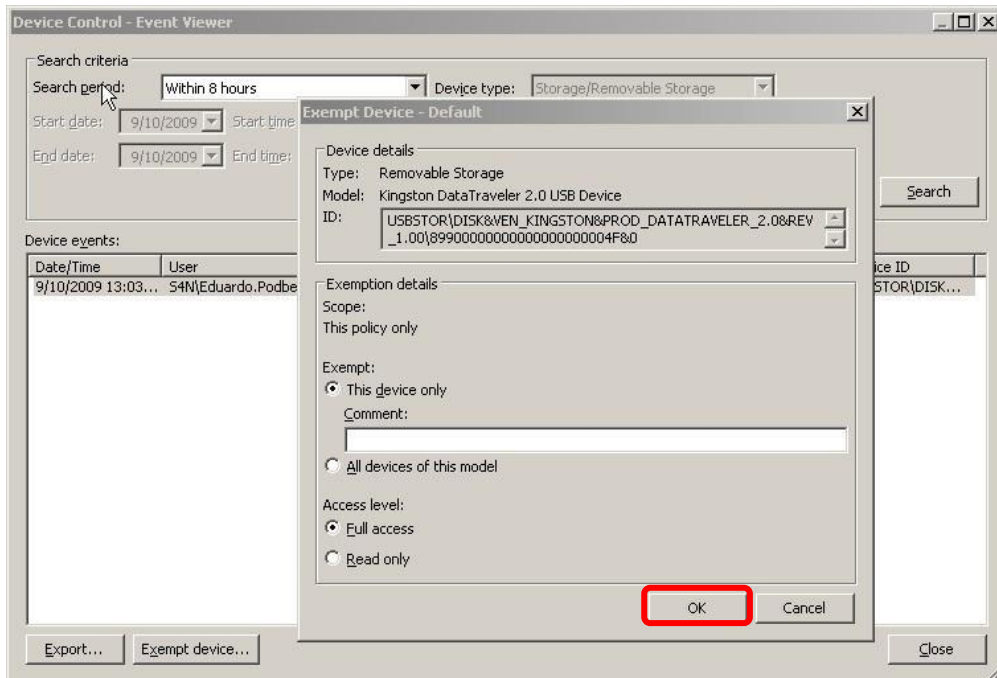
Dispositivos de armazenamento removíveis, *drives* de discos óticos e drives de disquete também podem ser preparados para prover acesso somente leitura.

1- Abra a política de device control

2- Selecione os tipos de dispositivos a serem controlados e na coluna **Status**, mude o status para a permissão desejada.

3- Para adicionar exceções, selecione o tipo de item a criar uma exceção (exemplo: caso for adicionar a exceção de um pendrive, selecione **Removable storage**) e clique em **Add exemption**

4- Faça a pesquisa pelo dispositivo, selecione o dispositivo e então clique em **Exempt device**:



5- Você pode adicionar este dispositivo como exceção (não será bloqueado) assim como todos dispositivos do mesmo modelo, clicando em **All devices of this model**.



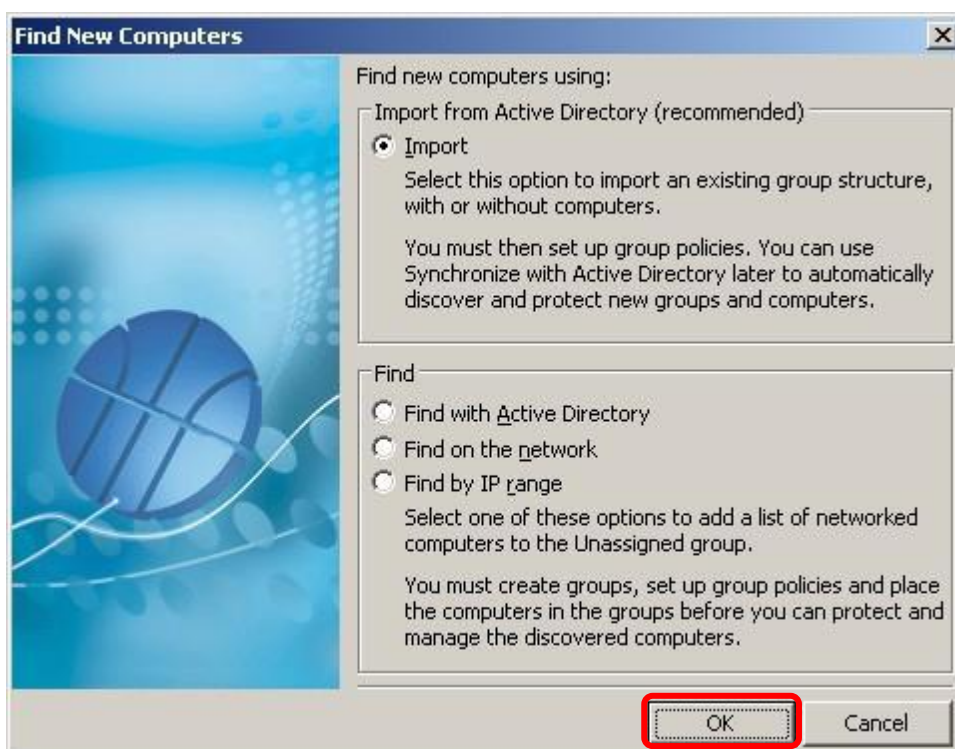
## Importando computadores

Neste tópico você irá aprender os métodos de localizar computadores:

- 1- Abra o Sophos Enterprise Console
- 2- Clique em **Find new computers**



- 3- Escolha o método de busca



- a. Pela opção **Import** você irá importar os grupos e computadores do seu Active Directory
- b. Pela opção **Find with Active Directory** você importa os computadores do seu Active Directory
- c. Pela opção **Find on the network** você localiza os computadores que estão em seu domínio ou em um grupo de trabalho (workgroup)
- d. Pela opção **Find by IP range** você localiza computadores em uma determinada faixa de IP

OBS: A diferença da opção **Importe** e da opção **Find with Active Directory**: Pela opção **Importe** você irá importar todos os grupos e computadores do Active Directory, já pela opção **Find with Active Directory** você irá importar somente os computadores.

4- Ao clicar em OK será necessário informar um usuário administrador da seguinte forma:

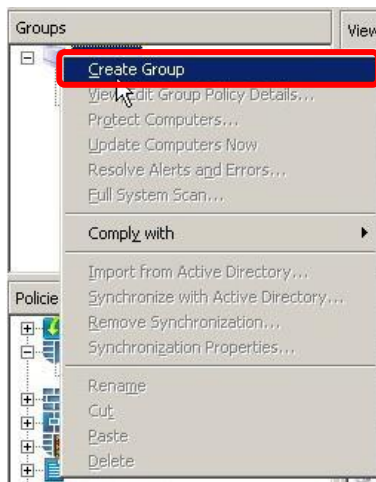
Para ambientes com domínio: domínio\usuário

Para ambientes sem domínio: \usuário

5- Após importar, os computadores poderão ser localizados no grupo **Unassigned** (com exceção das máquinas localizadas pela opção **Import** que já cria um grupo para as máquinas localizadas)

6- Crie um grupo e mova as máquinas para este grupo, para isto:

6.1- No quadro **Groups** clique com o botão direito na raiz e clique em **Create Group**:



6.2- Escolha um nome para o grupo

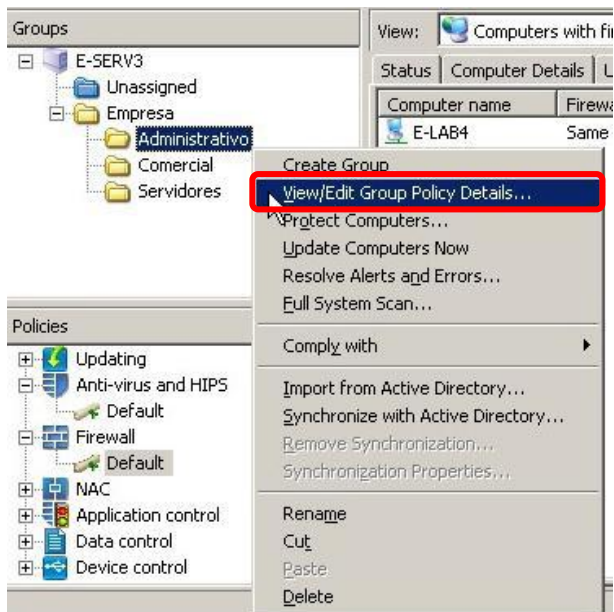
6.3- Na pasta **Unassigned**, selecione os computadores e arraste-os para o grupo criado

## Definindo regras para determinados grupos

Este tópico mostrará como definir regras para o grupo:

➤ Método 1:

- 1- Abra a console
- 2- Clique com o botão direito no grupo
- 3- Clique em **View/Edit Group Policy Details**



Agora apenas escolha quais políticas o grupo irá usar.

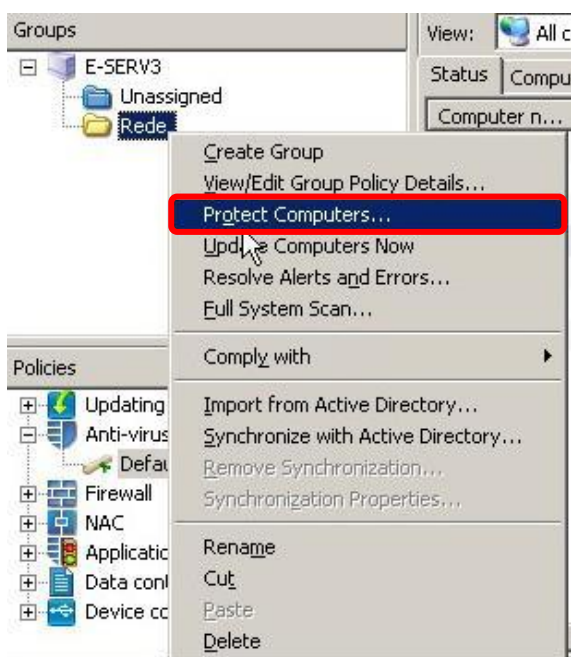
➤ Método 2:

- 1- Arraste a política para o grupo que irá usá-la.

## Instalando remotamente

Neste tópico você irá aprender a instalar o Sophos Antivírus pelo Sophos Enterprise Console, como citado no item “requisitos”, para realizar uma instalação remota revise as configurações citadas no manual “[Advanced startup](#)” (página 46 até 48, item 11.1.3 - Prepare for installation of anti-virus software), após ter revisado as configurações:

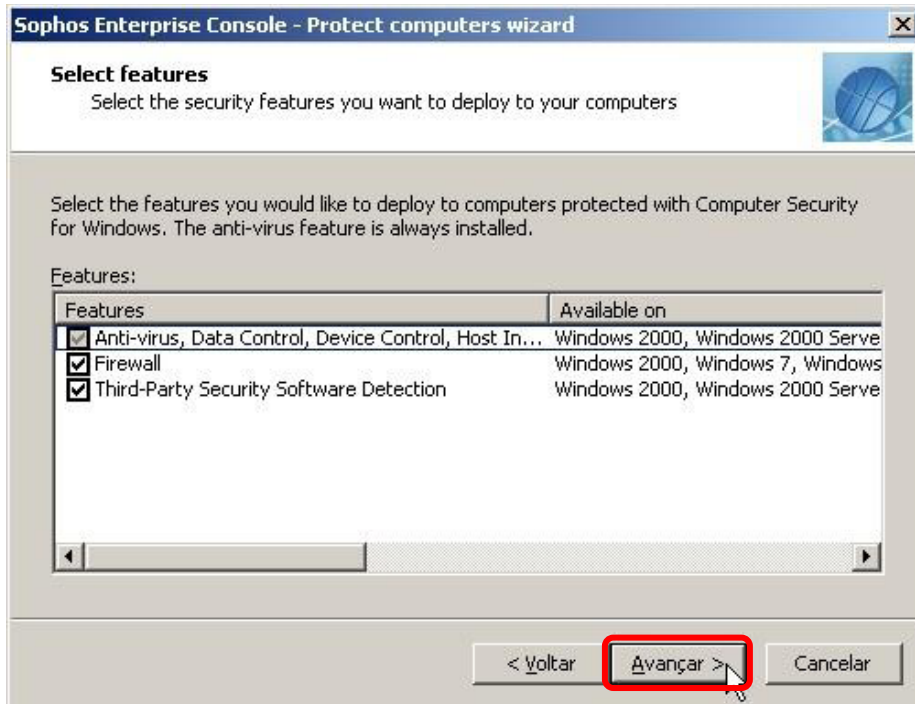
- 1- Abra a console
- 2- Selecione um grupo, uma máquina ou determinadas máquinas e clique com o botão direito
- 3- Clique em **Protect computers**



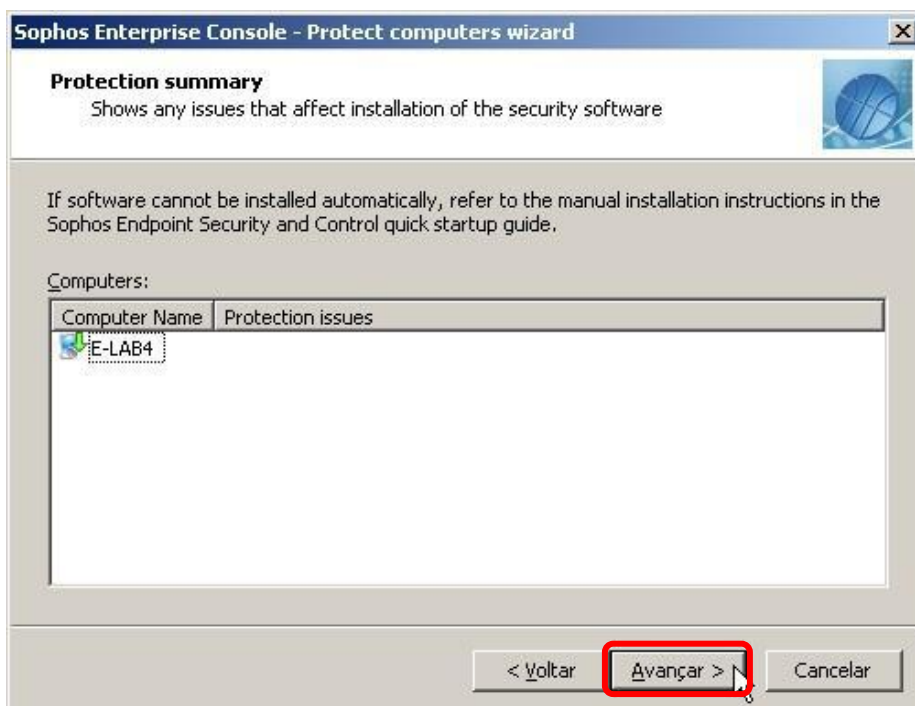
- 4- Clique em **Avançar**:



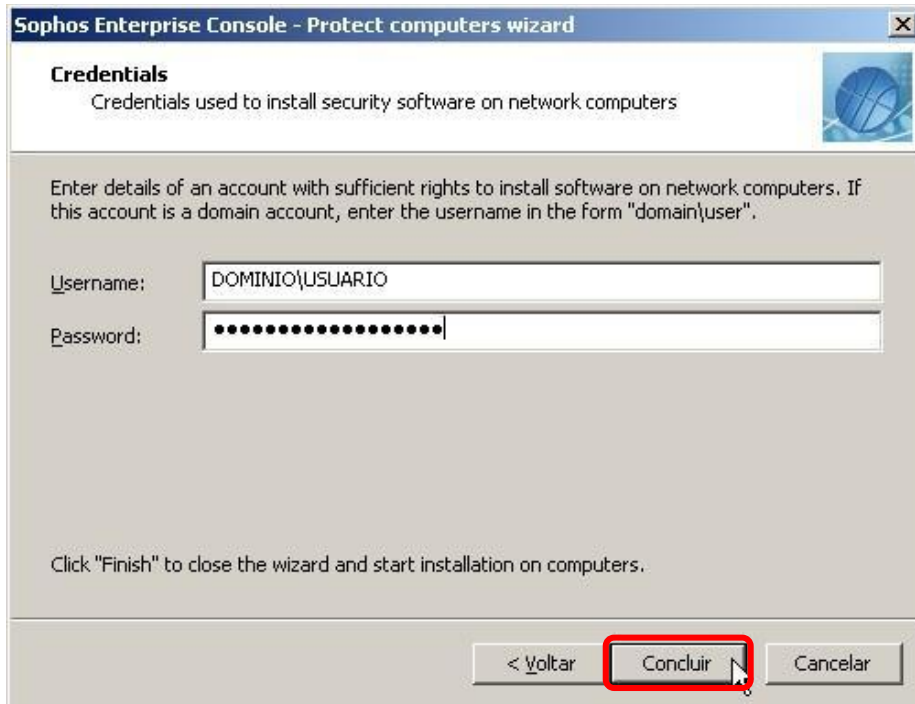
5- Seleccione as funções a serem instaladas:



6- Será listado o(s) computador(es) que o Sophos Enterprise Console irá instalar o Sophos Antivírus



7- Informe o usuário administrador no seguinte modelo:



Quando a seta estiver amarela, significa que o Sophos Enterprise Console está tentando localizar e autenticar o usuário no alvo.

Quando a seta esta verde significa que o Sophos Enterprise Console já localizou a máquina, autenticou e está iniciando a instalação.

Quando mudar para uma ampulheta o Sophos não teve problema na instalação está somente aguardando o retorno do Endpoint para a Console.

Dúvidas e sugestões, envie e-mail para [suporte@m3corp.com.br](mailto:suporte@m3corp.com.br) ou ligue (11) 4063-2087.