

## Tested Solution: Protecting a network with Sophos NAC Advanced and Allied Telesis Switches

Sophos NAC Advanced is a sophisticated Network Access Control implementation. It integrates tightly with other facilities on the Microsoft Server platform. This tested solution describes the steps involved in setting up Sophos NAC Advanced on a server running Microsoft Windows Server 2003, and the Allied Telesis switch configuration required to interoperate with this Sophos NAC implementation.

The description begins with a summary of the supporting applications that must be installed on the server. Then it moves on to the installation of the Sophos NAC server. The configuration of the NAC server to provide effective network protection is considered in some detail. Finally, the Allied Telesis switch configuration is provided, and the significant points in the configuration are discussed.

### Steps to setup and configure this Solution

- **Install the supporting Server features and applications**, see page 2
- **Install .NET Framework 2.0**, see page 8
- **Install SQL Server Express 2005**, see page 8
- **Install Microsoft WSE 3.0**, see page 11
- **Create remote access policies for the IAS server**, see page 13
- **Configure LAN switches as RADIUS client to the IAS server**, see page 17
- **Install Sophos NAC advanced**, see page 23
  - **Install the Sophos NAC SQL database**, see page 23
  - **Install the Sophos NAC application server**, see page 23
  - **Configure the Sophos NAC application**, see page 25
- **Create RADIUS enforcer access templates**, see page 27
  - **Create/configure profiles**, see page 29
  - **Create policies**, see page 31
- **Configure endpoint devices**, see page 33

For further information about NAC technology, and the NAC features available on Allied Telesis switches, see:

#### **“Advanced edge security with NAC”**

available from <http://www.alliedtelesis.com/resources/literature/literature.aspx?id=5>

## Installing the supporting server features and applications

To prepare a Windows 2003 server for installation of Sophos Advanced NAC, a number of Windows Server features must be enabled, and other applications installed.

For completeness, this solution description will assume that the server begins with a fresh installation of Microsoft Windows 2003, and will discuss all the steps required to go from that fresh installation to a state that is ready for Sophos Advanced NAC.

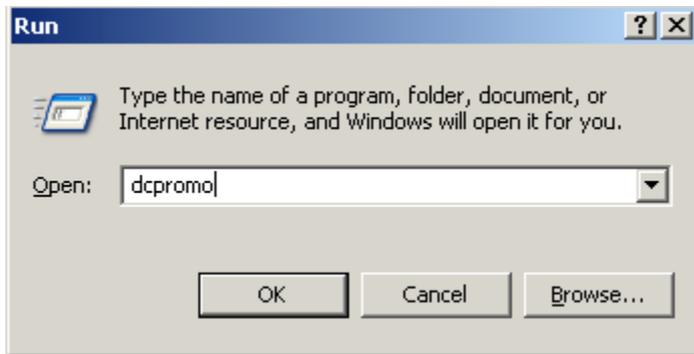
Many readers will skip some of these steps, as they will be starting with a server that has a number of these features already enabled. However, different servers will begin from different starting states, so to cover all cases; this document will describe all the required steps.

### Setting up the server as a Domain Controller

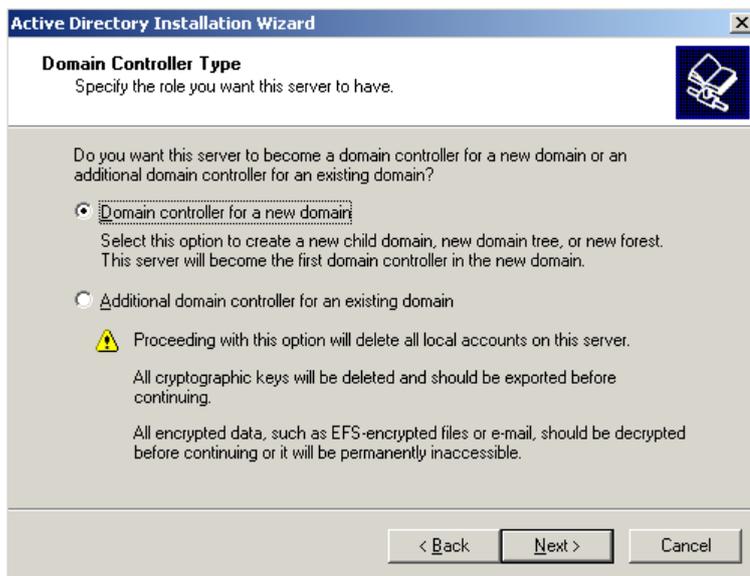
In this section, we will set up the server as a Domain Controller, and create a user account with the Active Directory user database. This will be called the NAC service account.

To begin the setting up of the Domain Controller feature:

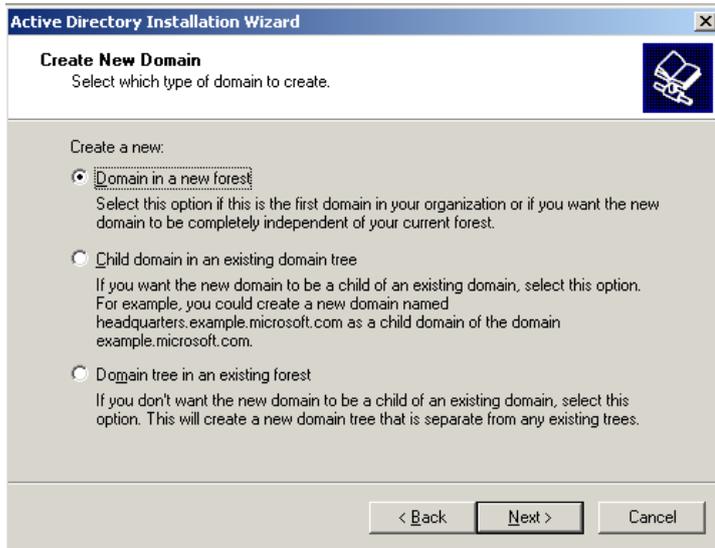
1. Run dcpromo.exe.



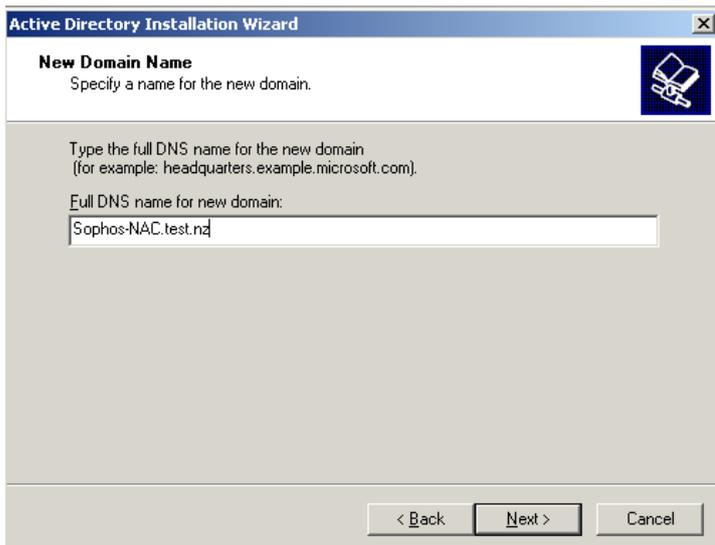
2. In this example, the server is the **Domain Controller for a new domain**.



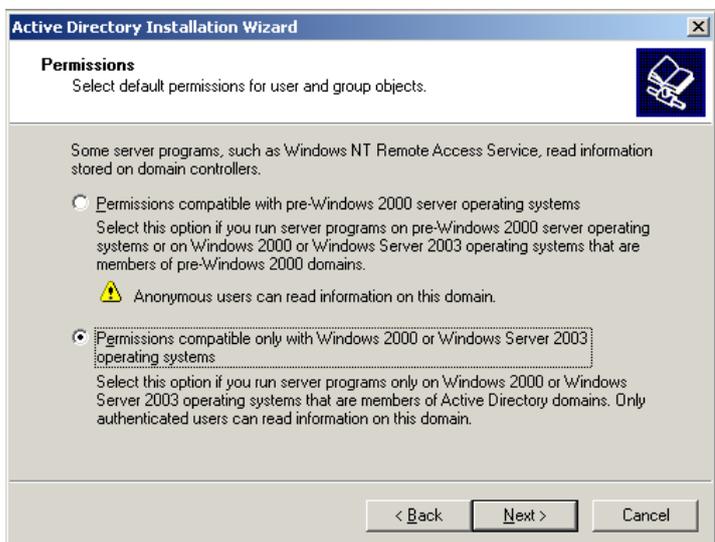
3. Select **Domain in a new forest.**



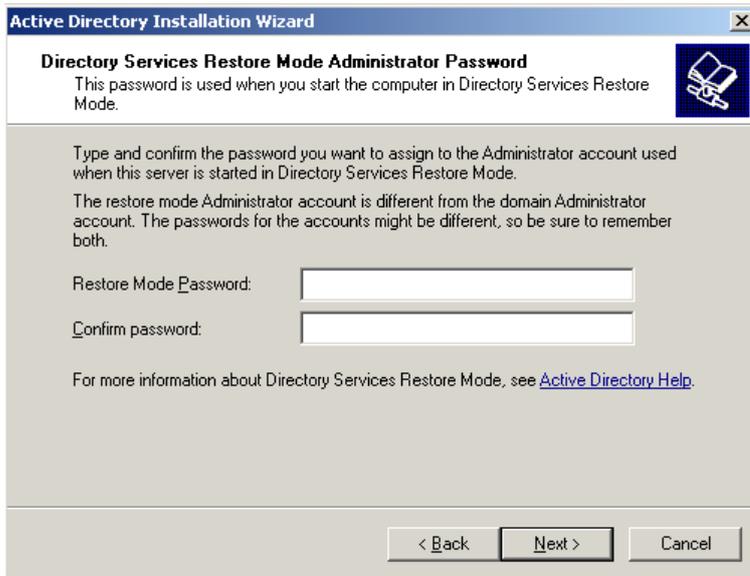
4. Provide a full **DNS name** for the server.



5. Select **Permissions** as required.



6. Set a **restore mode password** as required.

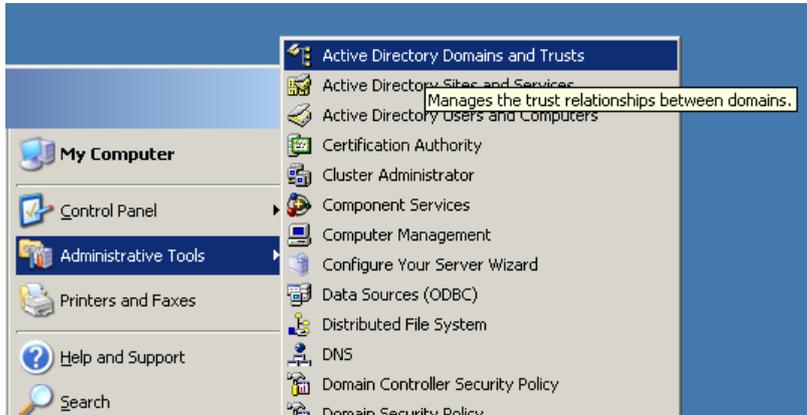


The screenshot shows a Windows dialog box titled "Active Directory Installation Wizard". The main heading is "Directory Services Restore Mode Administrator Password". Below the heading, it states: "This password is used when you start the computer in Directory Services Restore Mode." There is a small icon of a computer with a key. The main text area contains instructions: "Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode. The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both." Below this text are two input fields: "Restore Mode Password:" and "Confirm password:". At the bottom of the dialog box, there are three buttons: "< Back", "Next >", and "Cancel".

At this point, the enabling of the Domain Controller feature is complete. The next task is to **raise the functional level** of the Domain Controller.

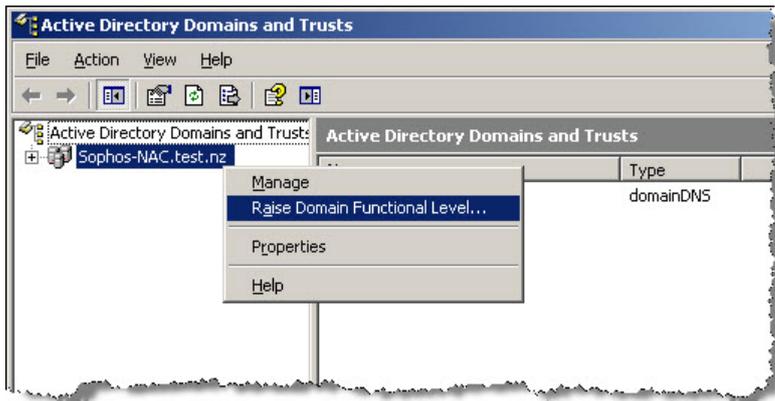
## Raising the functional level of the Domain Controller

1. Select **Administrative Tools > Active Directory Domains and Trusts**.

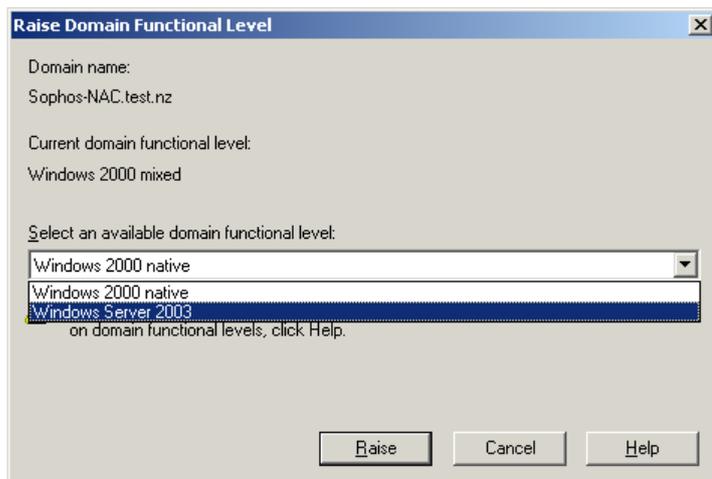


The server's name will appear in the list of domain servers in the left-hand pane.

2. Right-click on the server's name and select **Raise Domain Functional Level**.



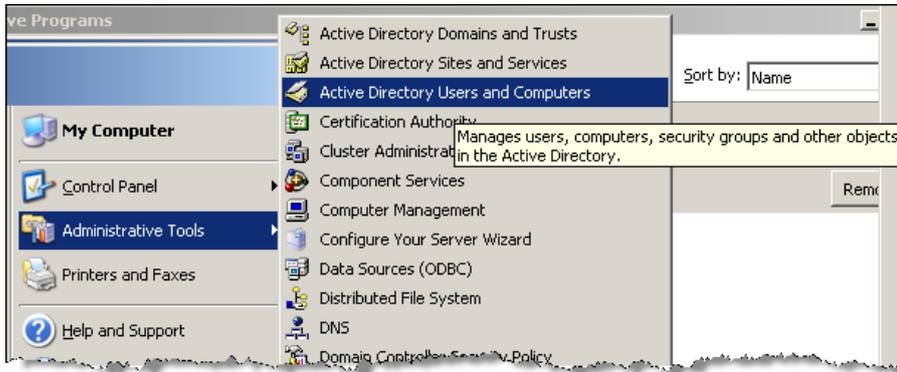
3. Set the domain functional level to **Windows Server 2003**.



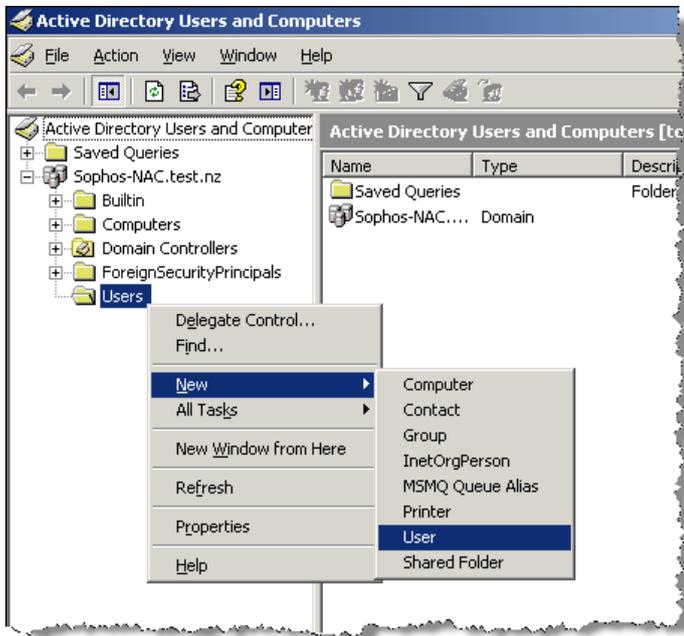
The final task in this section is to **create the NAC service user account**.

## Creating the NAC service user account

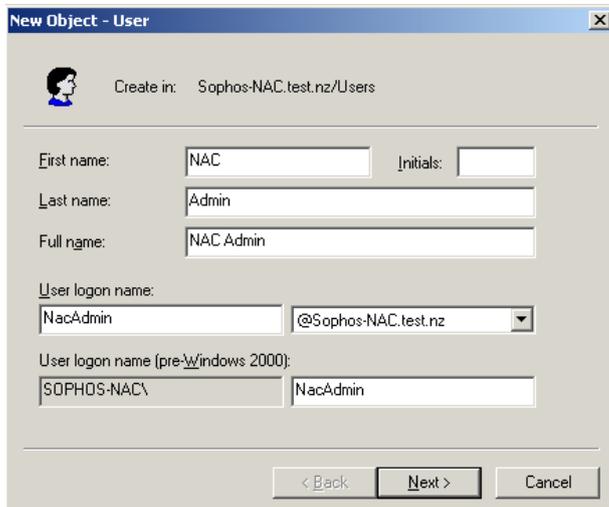
1. Select **Administrative Tools > Active Directory Users and Computers**.



2. Right-click on the **Users** menu item beneath the server's name. From the resulting pop-ups, choose **New >User**.



3. Provide the user with a **First name** and **Last name**, as below.



4. Provide the user with a **Password**, and the setup is complete.

New Object - User

Create in: Sophos-NAC.test.nz/Users

Password: [.....]

Confirm password: [.....]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back   Next >   Cancel

## Install the .NET Framework 2.0

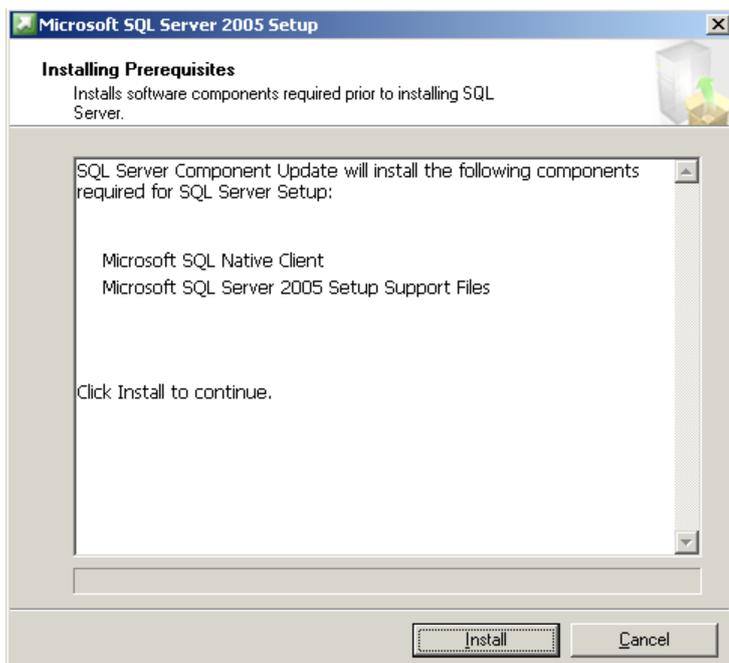
The .NET Framework 2.0 is a required pre-requisite for the SQL server express (which will be installed at the next step). The installer for this application is provided with the Sophos NAC Advanced distribution. It can also be downloaded from Microsoft.com.

This installation is very straightforward, simply run the installer, and you are guided through the installation, with no significant choices having to be made.

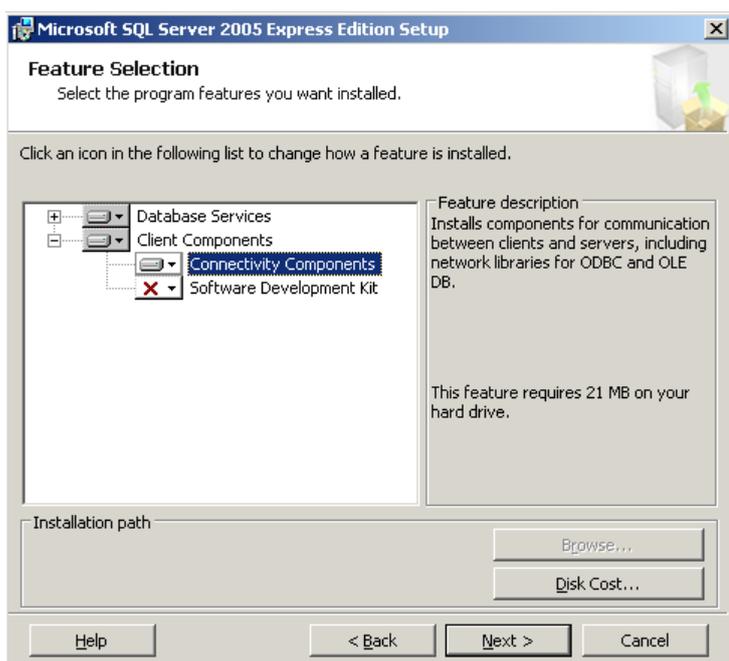
## Install SQL Server Express 2005

Sophos NAC Advanced will work with any standard SQL server. In this example, the SQL server being used is SQL server express 2005 – a light server that is freely available from Microsoft.com.

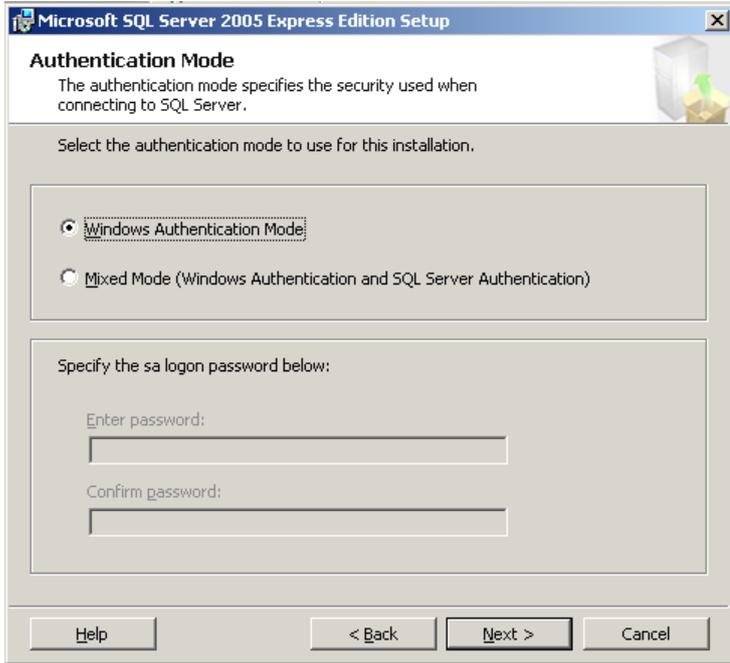
1. Run the installer, and you will be presented with the following opening dialog.



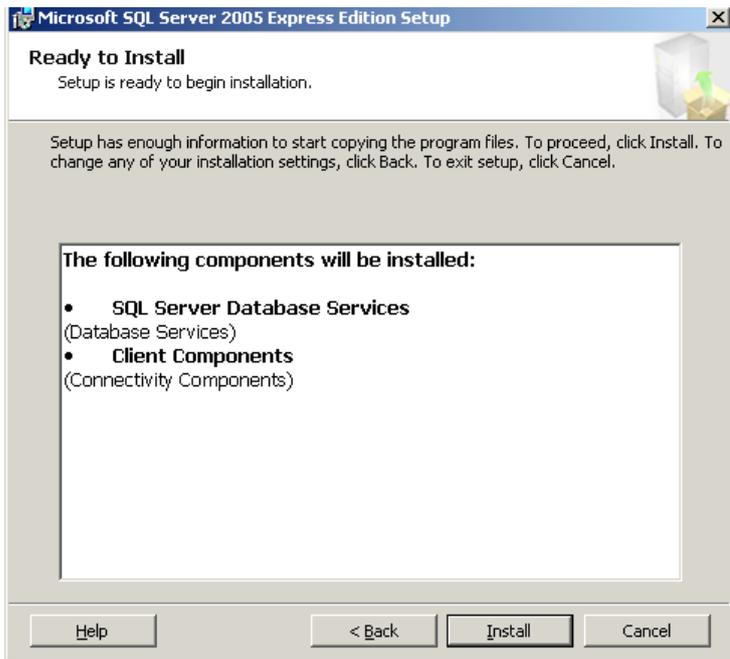
2. Click **Install**, and you will be offered the opportunity to decide which components to install. Leave this at the default setting.



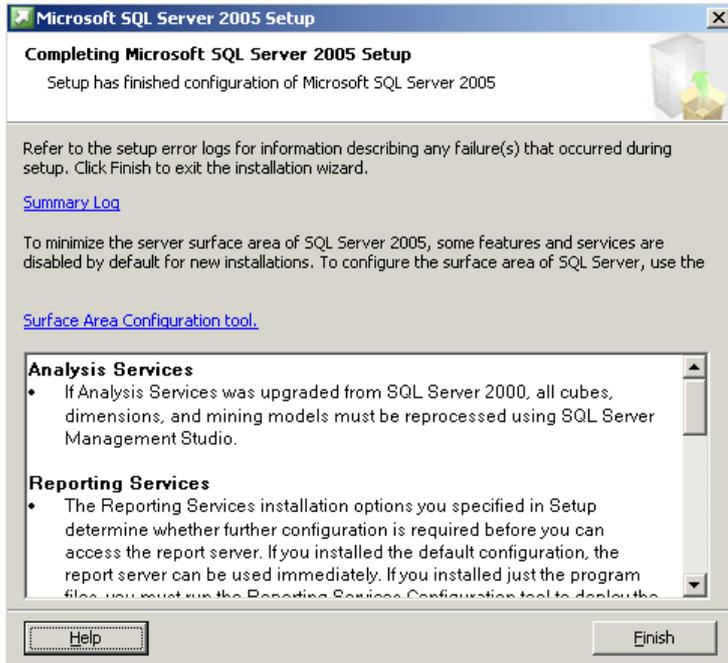
3. Ensure that the authentication mode is set to **Windows Authentication Mode**.



4. Click **Install** on the next dialog, and the SQL server will be installed.



5. When the installation is complete, you are presented with a summary.



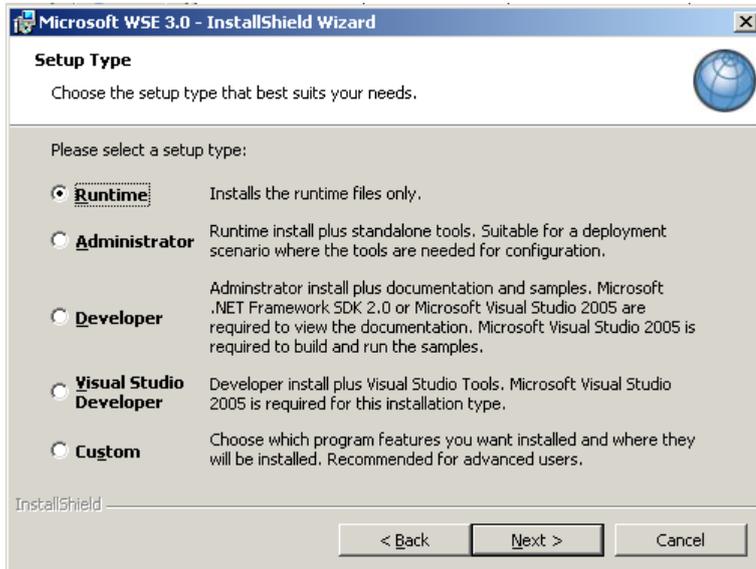
6. Click **Finish** and the SQL server will be installed.

## Install Microsoft WSE 3.0

The Microsoft Web Services Enhancement provides capabilities that are used by the Sophos NAC Web interface.

The installer for this is provided on the Sophos NAC Advanced distribution CD, and can also be downloaded from Microsoft.com. The installation of this software is very straightforward. The only choice that needs to be made is on the second dialog, where you need to choose the setup type.

Choose to make a **Runtime** setup.



## Ensure that ASP.NET v2.x is an allowed Web Service Extension

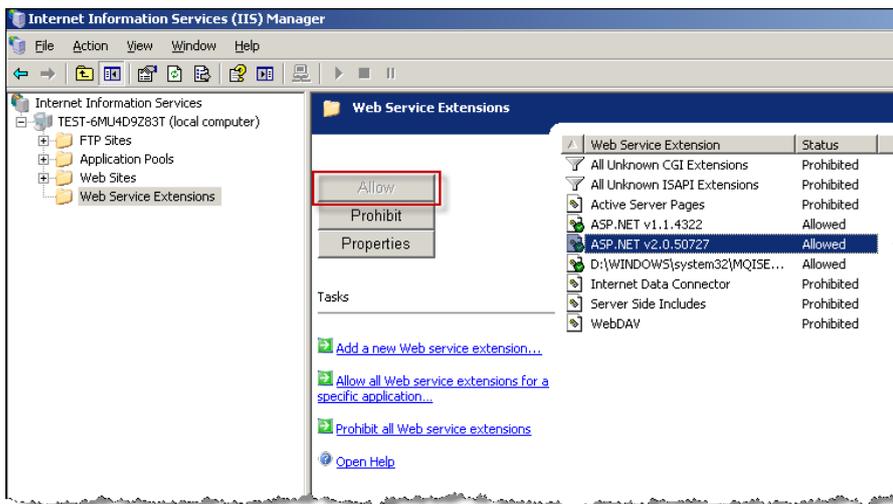
The operation of Sophos NAC Advanced requires that ASPNET is an allowed Web Service Extension. By default, it is not an allowed extension, so you need to set it as such.

### 1. Select **Administrative Tools > IIS Manager**.



### 2. Within the IIS Manager, choose **Web Services Extensions** in the left-hand pane. A list of the Web Services Extensions is displayed.

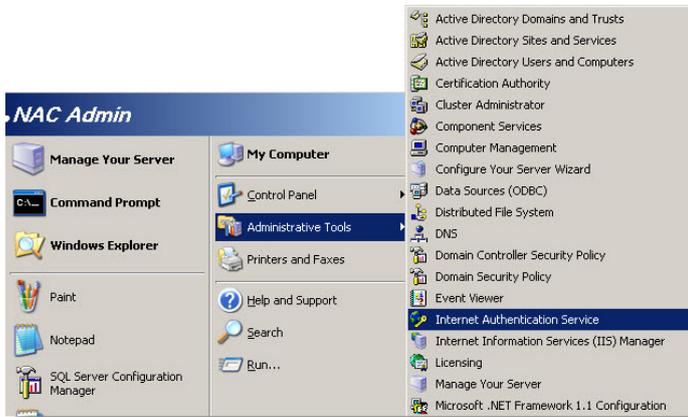
1. Highlight **ASP.NET v2.xxxxx**.
2. Click the **Allow** button.



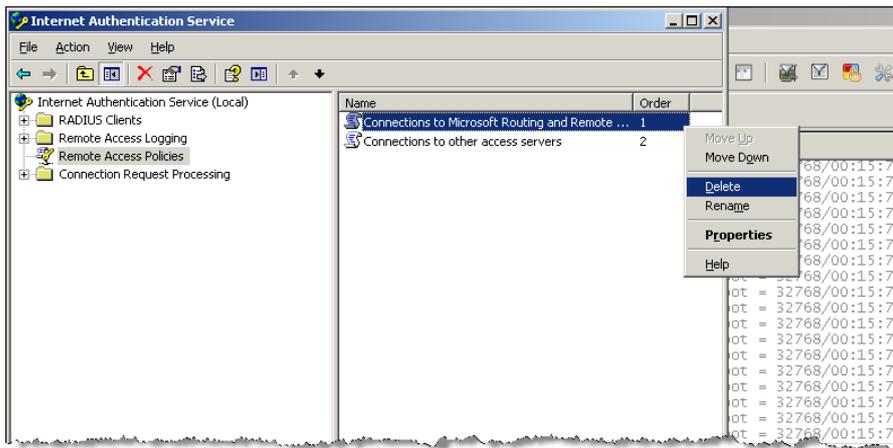
## Create Remote Access policies for the IAS server

Central to the operation of NAC is the RADIUS authentication of 802.1x supplicants. Sophos NAC Advanced integrates with the IAS server as the RADIUS server. The IAS server needs to be set up with a remote access policy for 802.1x supplicants. Separately, it will need another remote access policy that is used directly by the NAC agents in the End-Point PCs to register themselves to the NAC server when they are first installed.

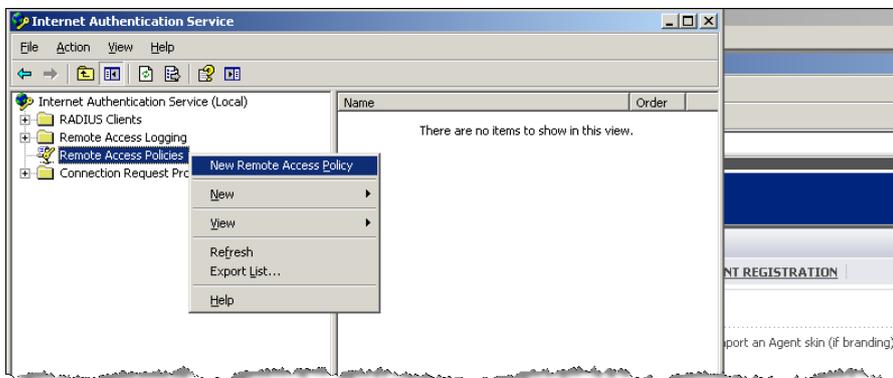
1. Select **Administrative Tools > Internet Authentication**.



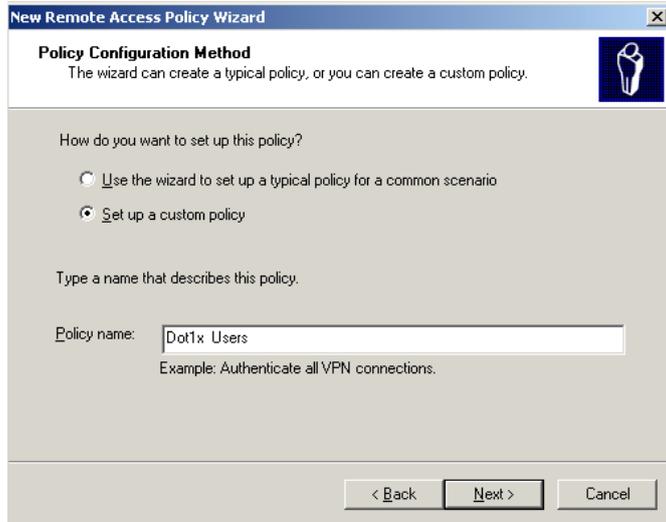
2. Within the IAS manager, select **Remote Access Policies** within the left-hand pane. You may wish to begin by deleting the default remote access polices that are listed in the right-hand pane.



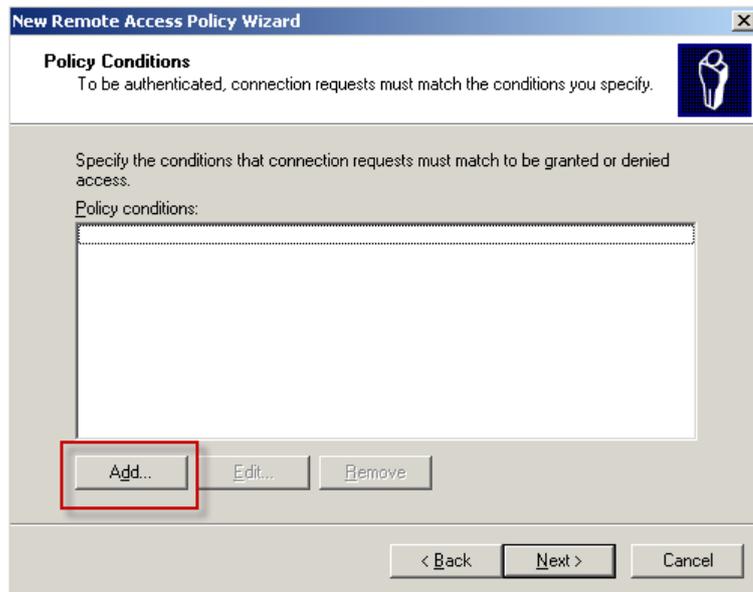
3. Right-click on **Remote Access Policies**, and select **New Remote Access Policy**.



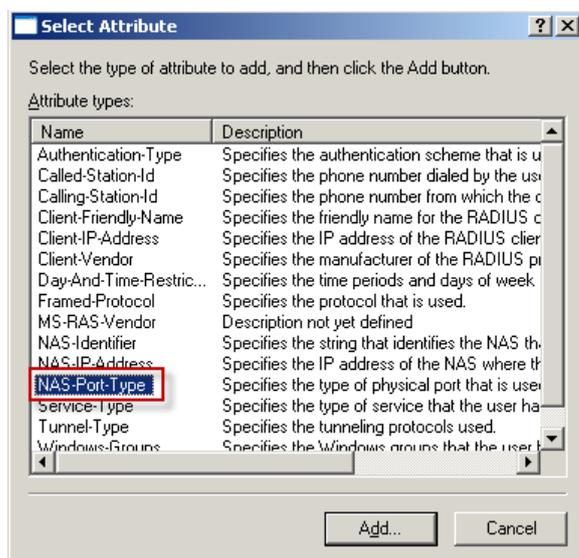
4. Select **Set up a custom policy**, and give it a name like **Dot1x Users**.



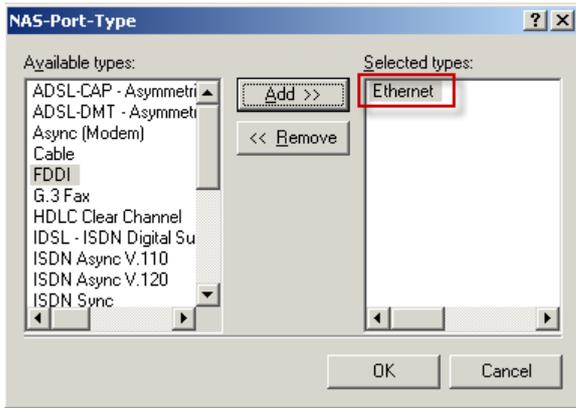
5. Choose to **Add** a policy condition.



6. Select the attribute **NAS-Port-Type**.

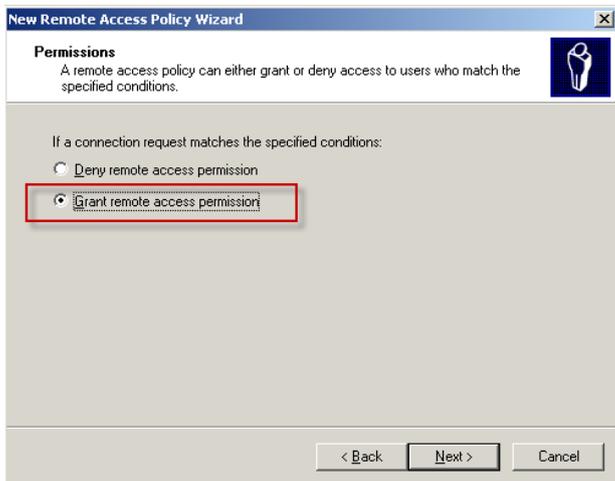


7. Select **Ethernet** as the value that **NAS-Port-Type** must match.



8. Click **OK**.

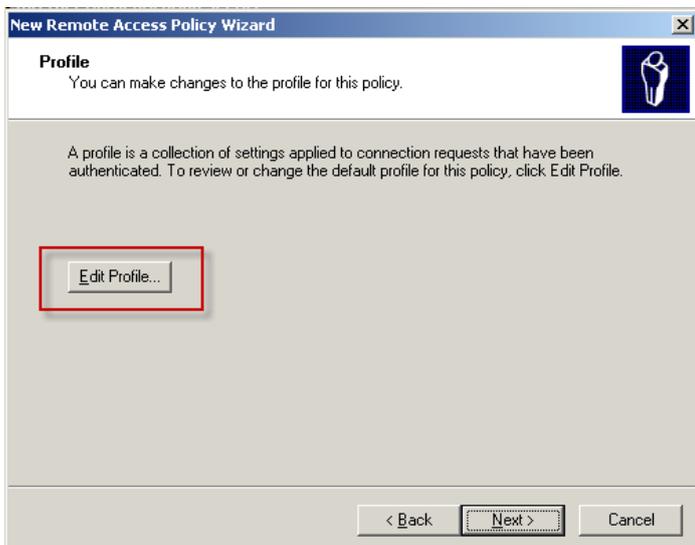
The action of the policy is to **grant remote access permission to users**.



9. Click **Next**.

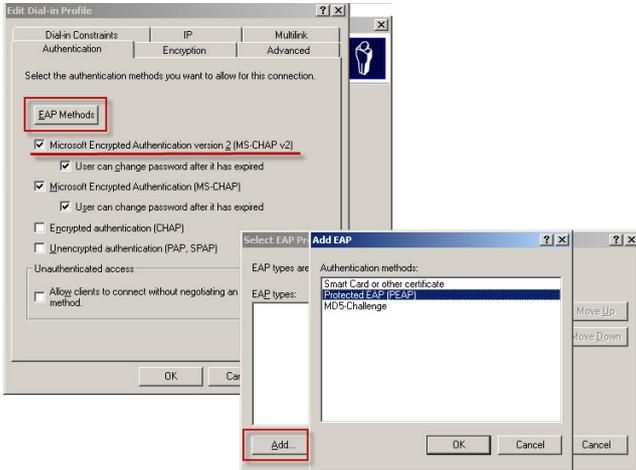
You now need to edit the profile for this access policy.

10. Click **Edit Profile...**



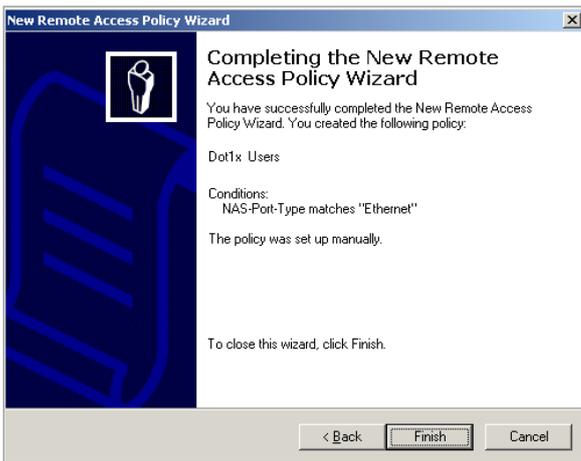
The aspect of the profile to be configured is the authentication methods.

- In the **Authentication** tab, click the **EAP Methods** button, and add EAP method **PEAP**.
- In the main body of the **Authentication** tab, ensure that **MS-CHAPv2** is ticked.



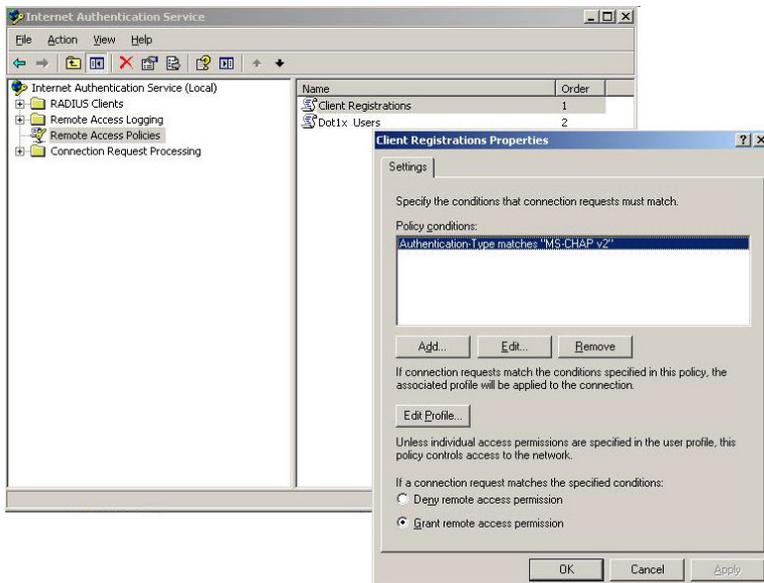
- Click **OK**.

The creation and configuration of the Access Policy is now complete.



## To create the Remote Access Policy for agent registration

Create a simple policy that has the condition that the Authentication Type is **MS-CHAPv2**.



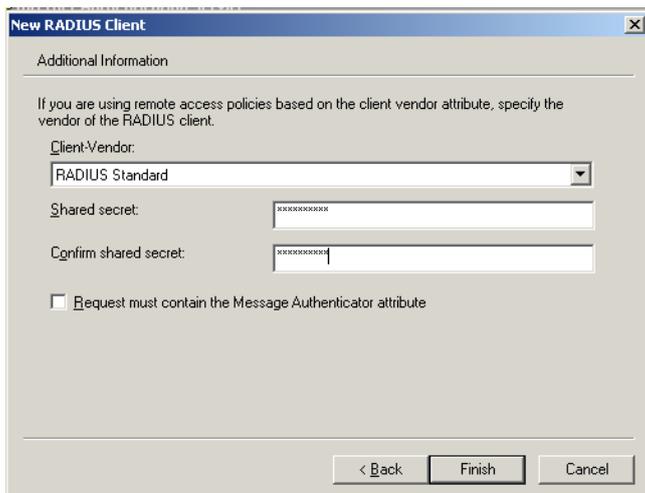
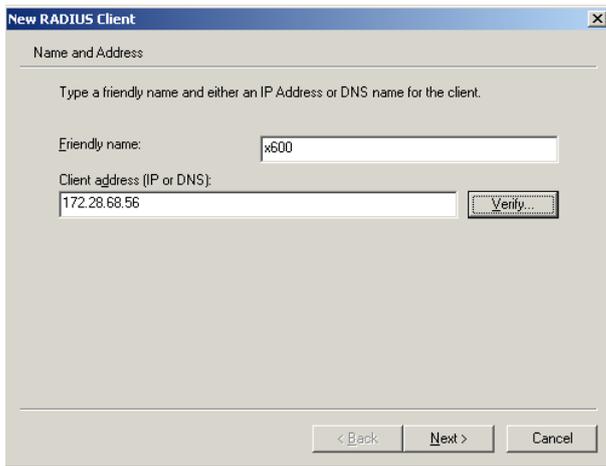
## Configure LAN switches as RADIUS client to the IAS server

The IAS server needs to be configured with the details of the LAN switches that will operate as the 802.1x authenticators.

1. From within the IAS manager, right-click on **RADIUS Clients** in the left-hand pane, and choose **New RADIUS Client**.



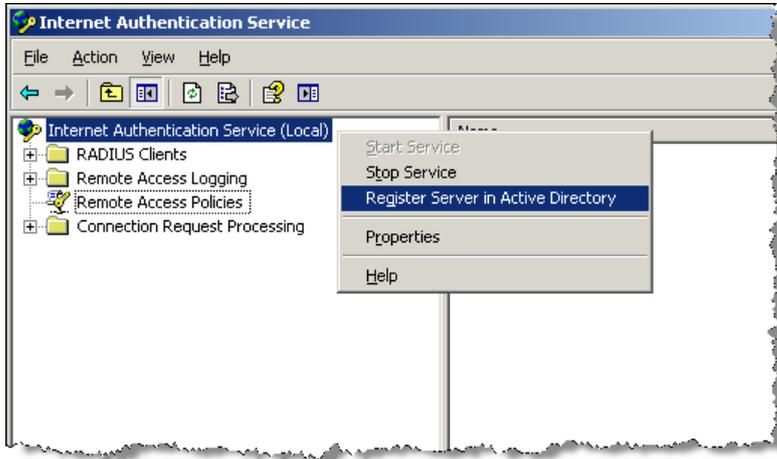
2. Enter the details of your Radius clients (802.1x authenticator switches).



## Register IAS with Active Directory

So that IAS can use Active Directory as a source of user credentials, it needs to be registered with Active Directory.

Right-click on **Internet Authentication Service (Local)** in the left-hand pane of the IAS manager; and choose **Register Server in Active Directory**.



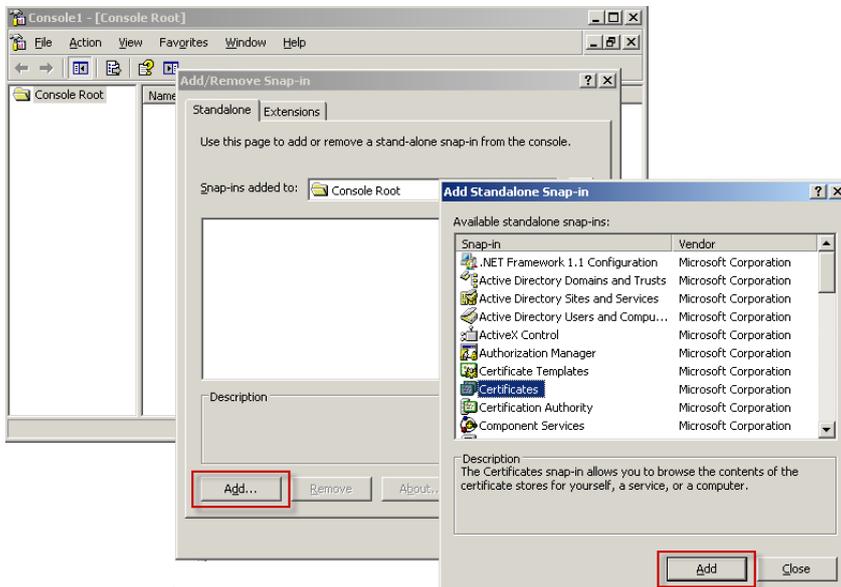
## Install a Certificate into the Web Server

A number of the tasks performed by Sophos NAC Advanced are achieved via a secure Web interface. So, the Web Service running on the server must be capable of secure web connections; therefore it must possess an X.509 certificate.

First, a certificate must be obtained and brought into the Server's Certificate Store.

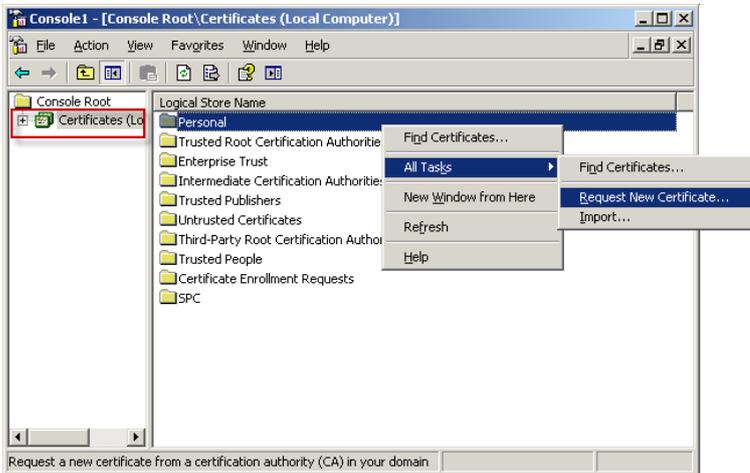
### To add a certificate into the Certificate Store:

1. Begin by running **mmc** to bring up the windows console on the server.
2. Add the certificates snap-in into the console. To do this:
  - a. Right-click on **Console Root** in the left-hand pane of the console, and choose **Add/Remove Snap-in** from the resulting **pop-up menu**.
  - b. Click **Add** in the resulting dialog. You will then be presented with a list of available Snap-ins to add.
  - c. Select **Certificates** from this list.
  - d. Click **Add**.



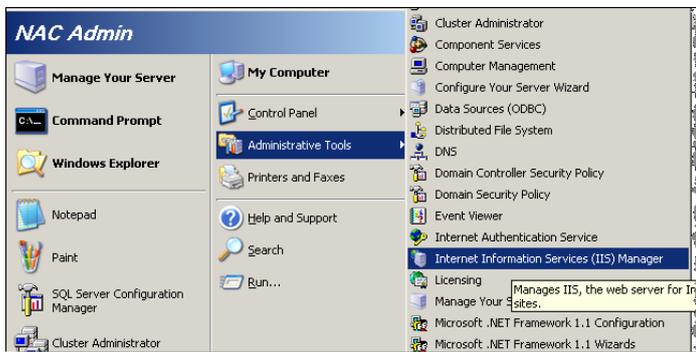
3. Once the Snap-in is in place, it can be used to add a certificate to the store.

- a. Select **Certificates** in the left-hand pane of the Console,
- b. Right-click on the **Personal** store in the right-hand pane and select **All Tasks > Request New Certificate...** to request a certificate from a Certificate Server (if you have a Certificate Authority set up in your network) or to import a certificate that has been supplied to you as PKCS or DER file. (The process of obtaining certificates or certificate servers is beyond the scope of this document).

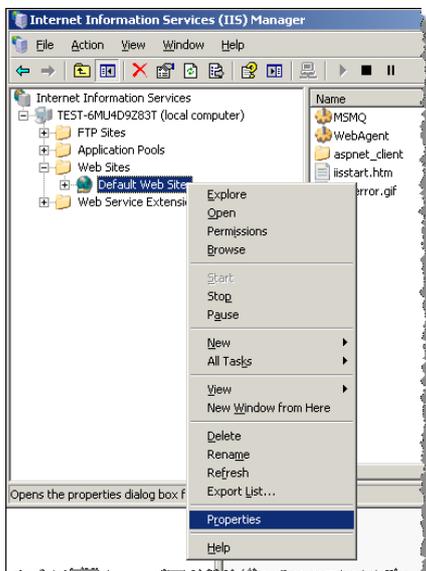


Once the certificate is in the store, the Web server needs to use this as its server certificate.

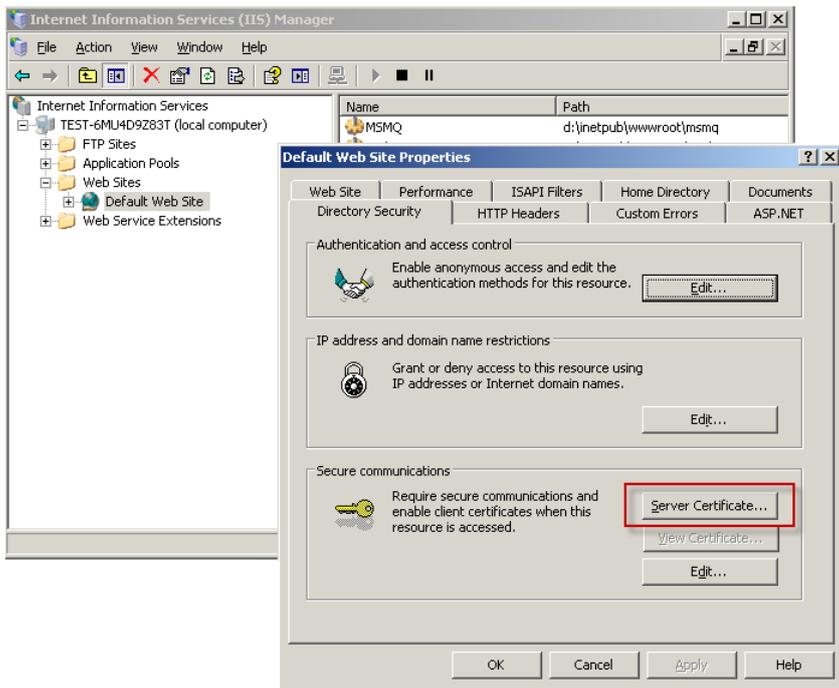
4. Run the IIS manager from the **Administrative Tools** menu.



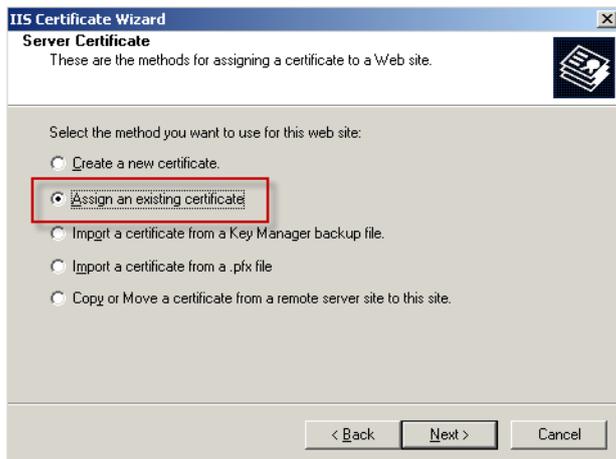
5. Select Default **Web Site > Properties**.



6. Click **Server Certificate**.

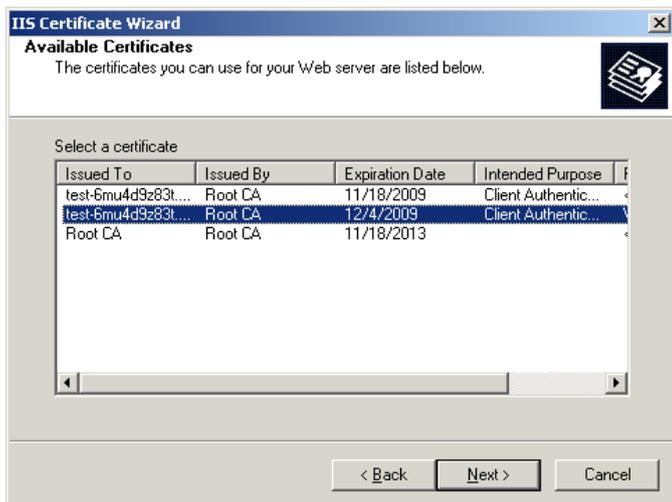


7. Select **Assign an existing certificate**.

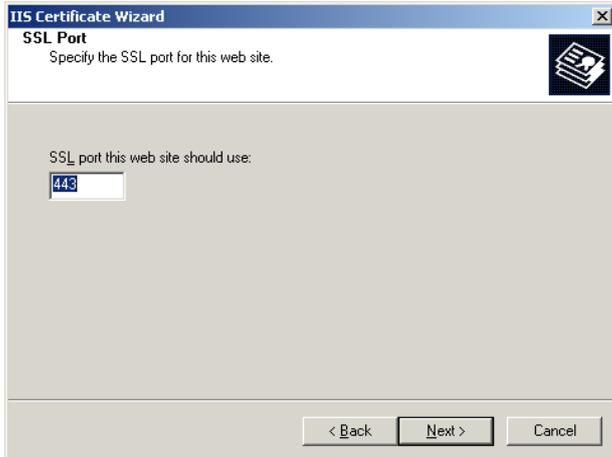


You will be presented with a list of the certificates present in your certificate store.

8. Choose the **certificate** you intended for use as your Web Server certificate.



It is best to set the TCP port for the secure connections at the default value of **443**.



9. Click **Next**.

10. Click **Finish** to complete the certificate installation.



## Install Sophos Advanced NAC

The supporting features and applications are now sufficiently in place to allow Sophos NAC Advanced to be installed.

First, the Sophos NAC SQL database must be installed, and then the NAC application itself can be installed.

### Install the Sophos NAC SQL database

The Sophos NAC SQL database is installed by running the file **Sophos NAC SQLServerInstall.msi** from the Sophos NAC Advanced distribution. In preparation for installation, the installer needs to know the details of the SQL server that has been installed.

In this example, we installed SQL server express. This is identified to the database installer as `.\SQLEXPRESS`.

Recall, also, that we specified Windows Authentication when installing the SQL server. So, that authentication method needs to be chosen here in the database installation.



The database installation also needs to know the details of the NAC Service User Account that was created in Active Directory. Enter these details in the second dialog of database installation wizard.

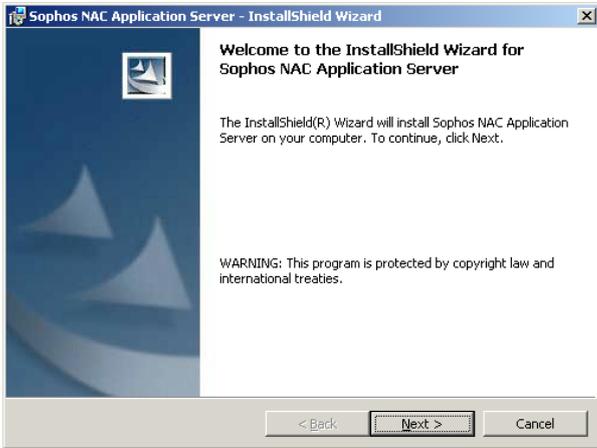


From there, the Installer simply proceeds to install the database.

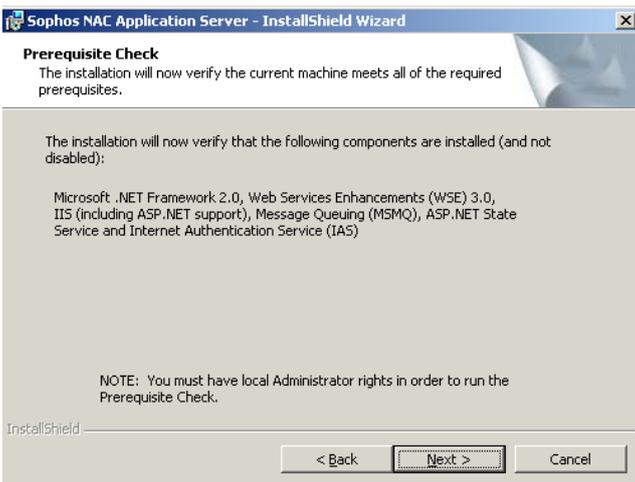
## Install the Sophos NAC Application Server

The Sophos NAC application server itself can now be installed.

- This is initiated by using the file **Sophos NAC Application Server.msi** in the Sophos NAC distribution.



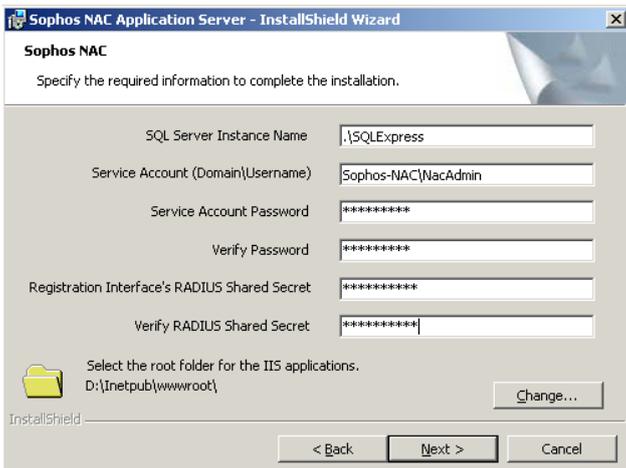
The installer begins by checking for all the supporting applications and features.



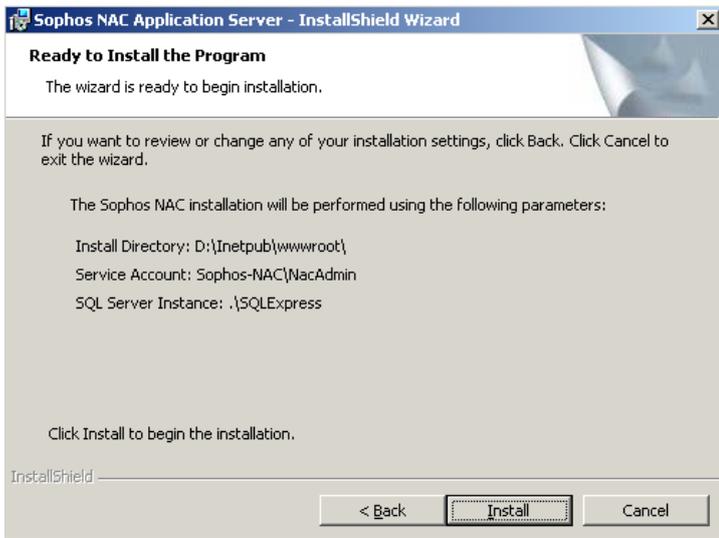
- Click **Next** to continue.

The SQL server and NAC Service Account details need to be provided again.

- In addition, a **RADIUS Shared Secret** needs to be specified that is used by the Agent software within the end-point PCs when they register themselves to the NAC server.



- Click **Install** to begin.



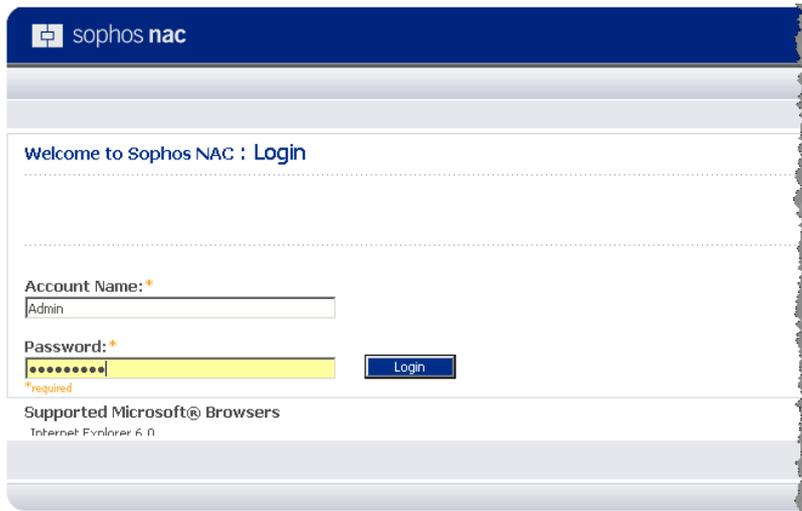
## Configuring the Sophos NAC application

Once the application server has completed its installation, you can then start configuring your security policy. The Application Server does not have a native interface, but is accessed entirely via a web interface.

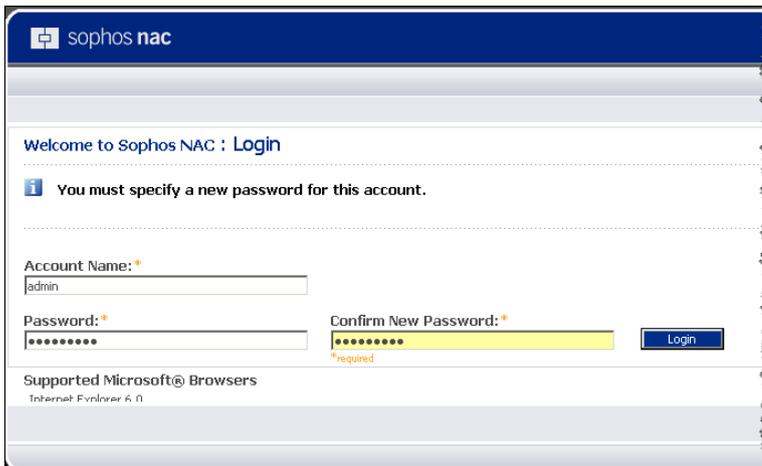
### Logging in to the Application

To access this web interface:

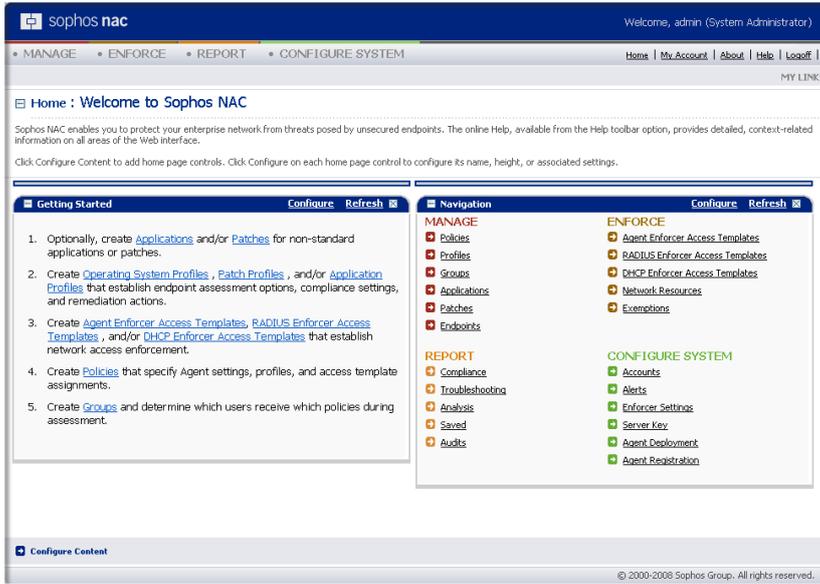
1. Browse to: **http://<ip address server>/SophosNAC**. The Web interface Logon page displays:



2. Type **Admin** in the **Account Name** field and a password of your choice in the **Password** field.
3. Click **Login**.
4. The first time you access the Web interface you are required to change the password.



You are then given access to the application.



There are a number of elements within the application that must now be configured in order to create a NAC solution. There is no fixed order in which these tasks must be performed (although some, certainly, must be performed before others.) The order presented below is reasonably logical.

## Create RADIUS Enforcer Access Templates

The access templates define the RADIUS attributes that will be sent to end devices when their health check is complete. Initially, you are presented with the details of the existing default Access Templates. There is a template that Allows all users, and one that Denies all users.

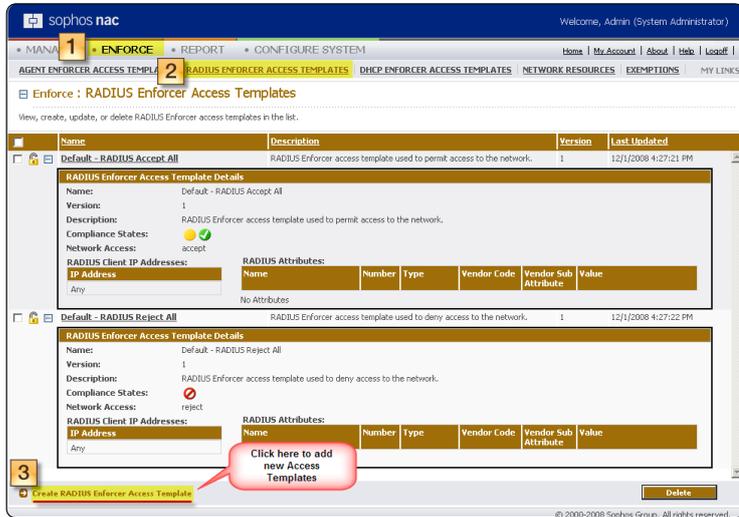
Whilst these Access Templates are not likely to be of much use for your NAC solution, it is worth taking a look at the structure of the templates, to become acquainted with what elements comprise a RADIUS Enforcer Access Template.

There are four significant items in the Template details:

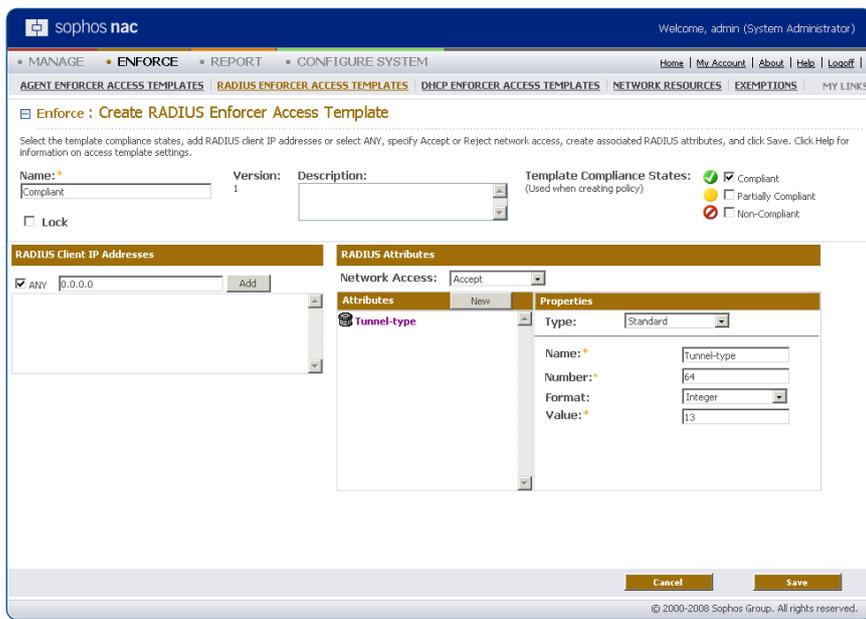
- **Compliance State** – This indicates which sort of end-points this Access Template will be applied to. This will become clearer when the Policies are described, below, but in summary, the NAC server determines the level of an End-Point's compliance with the Health policy, and then decides which Access Templates can be applied to the End-Point.
  - The Compliance State can take values **Compliant**, **Partially Compliant**, and **Non-Compliant**. Again, the process by which the server decides which state an End-Point is in will be discussed later on.
- **Network Access** – This indicates whether a RADIUS-Accept message or a RADIUS-Reject message will be sent to the End-Point at the end of the RADIUS negotiation.
- **RADIUS Client IP Addresses** – This indicates which RADIUS clients (i.e. 802.1x authenticator LAN switches) this Access Template applies to. If a RADIUS request comes from a RADIUS client that is not within the range(s) of addresses defined here, then this Access Template cannot apply to that request.
- **RADIUS Attributes** – This is a list of attributes that will be sent to the RADIUS client if the RADIUS request is accepted. Typically, the attributes will be used to dynamically allocate a VLAN ID.

To create new RADIUS Enforcer Access templates

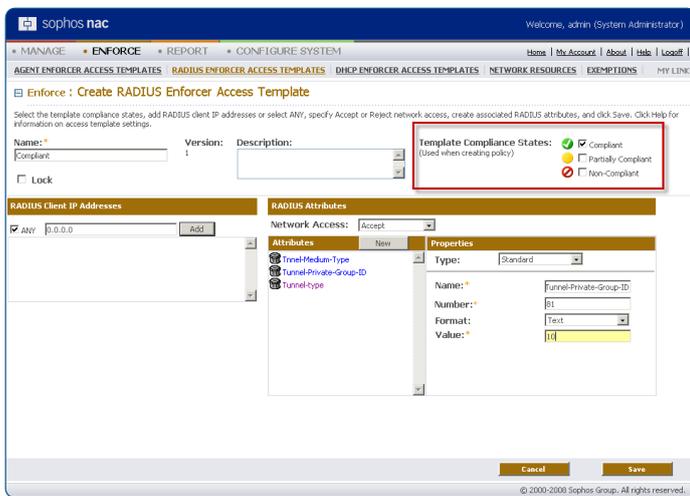
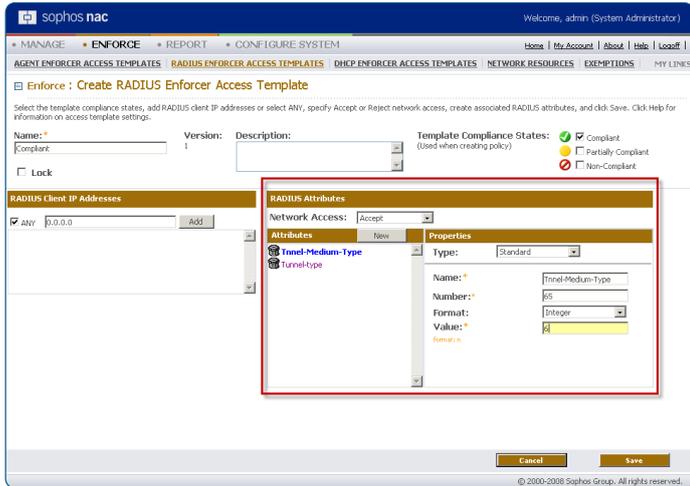
1. Select **Enforce** from the menu across the top of the application window.
2. Select **Radius Enforcer Access Templates** from the second-layer bar menu that is then created.
3. Select **Create RADIUS Enforcer Access Template**.



This will provide you with an interface within which you can define the attributes of the new template.



- You can decide on the **Name** and **Description** to give the template.
- You have a choice of which **Compliance States** the template will apply to – you can choose any combination of the 3 states.
- You can add ranges of applicable **RADIUS Client IP Addresses**, or leave the client address setting at its default value of 'ANY'.
- The area of the template you are most likely to configure is the **RADIUS Attributes**. The first item that can be set in that section is the choice as to whether or not users to whom this template is applied are to be given access to the network. Then you can define the attributes that will be allocated to the RADIUS client if the supplicant is to be given network access. To dynamically allocate a VLAN ID to an Allied Telesis switch, you must set the following three attributes:
  - **Tunnel-type** is set to VLAN (value=13)
  - **Tunnel-Medium-Type** is set to IEEE 802 Ethernet (value=6)
  - **Tunnel-Private-Group-ID** is set to the VLAN ID that is to be allocated to the RADIUS Client



For the **Template Compliance States**, you will probably wish to create different templates for Compliant, Partially-Compliant and Non-Compliant end-points. Possibly, Partially-Compliant and Non-Compliant end-points will be assigned to a remediation VLAN.

Also, for compliant end-points, you may have different access templates for different RADIUS clients – as the different clients may be in different parts of the network, where different VLANs are in use.

**Create** and **save** whatever RADIUS Enforcer Access Templates are required for your NAC solution.

## Creating/Configuring profiles

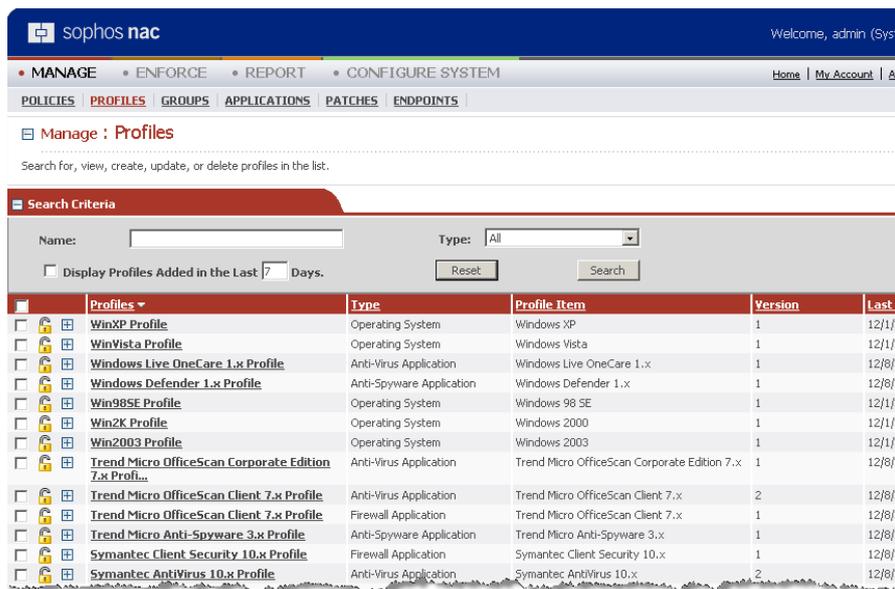
Profiles sit at the heart of defining the health policy for end-point devices.

Profiles are the individual items that are checked when the health status of a device is being assessed. They are things like: which virus scanner is installed? How up-to-date is its virus pattern database? What operating system security patches are installed? Etc.

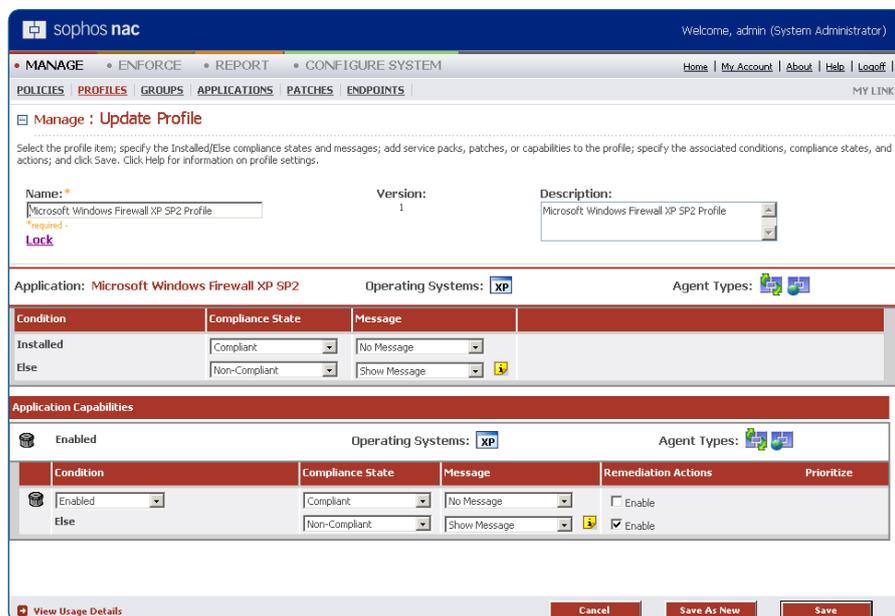
To access the profile editing interface, choose **Manage** from the menu along the top of the application interface. Then choose **Profiles** from the drop-down menu.



You will be presented with a large list of pre-defined profiles:



From there, you can either choose to create a new profile, or click on an existing profile to edit it. For example, you can see below that the Profile for the Windows Firewall under XP SP2 is being edited. The profile is effectively a series of properties to check in relation to this application – is it installed, is it enabled? – and decisions to make based on the answers those questions. The decisions can be to declare the client device compliant or non-compliant, whether to present the user a message in relation to this decision, and whether to take remedial action.



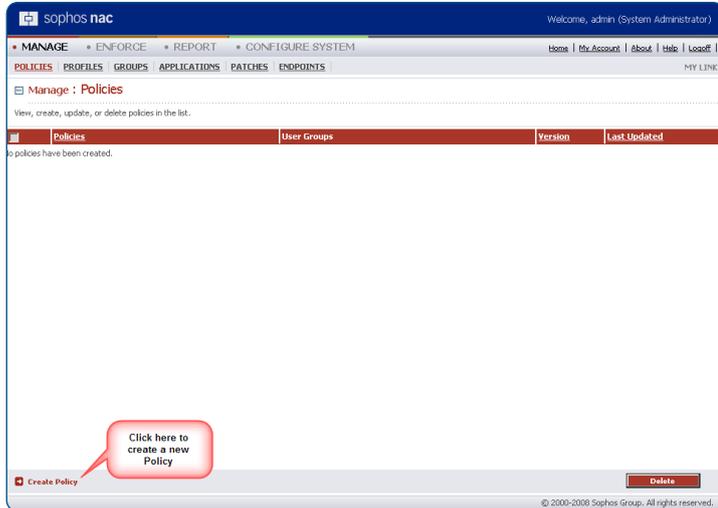
The default list of profiles in the application is quite extensive, and has chosen sensible default settings, so it is quite possible that you will not have to make any changes or additions to the profiles.

## Creating policies

A policy combines a set of profiles together; to create a definition of what will constitute a health-check of endpoint devices.

You can edit policies via the **Manage** menu. The opening screen lists all the currently existing policies. By default, no policies exist.

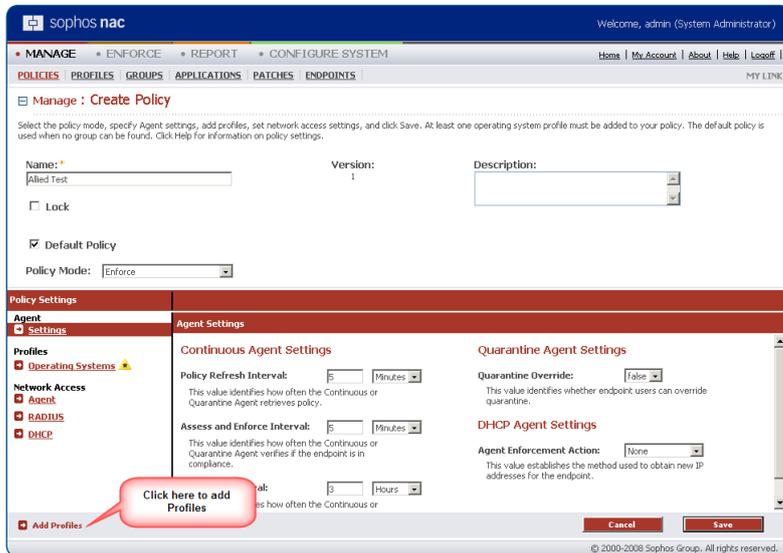
To create a new Policy, click on **Create Policy**, near the bottom of the window.

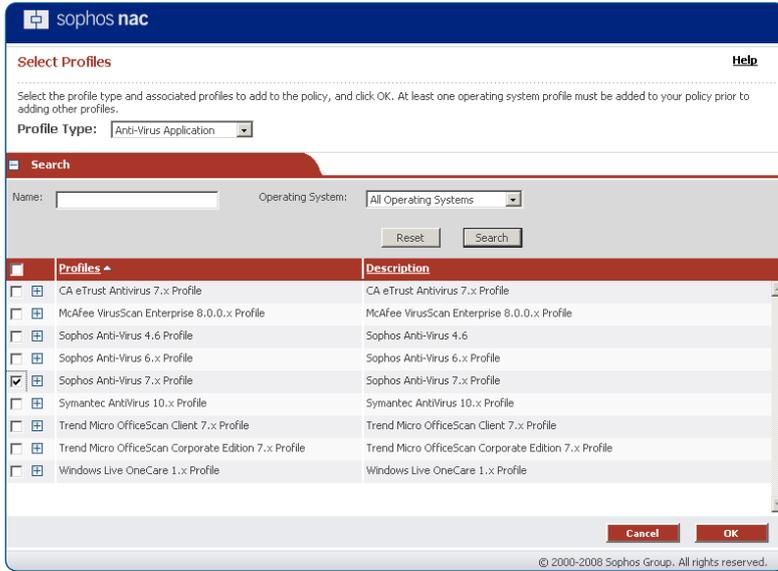


The central task in creating a Policy is that of adding the profiles that define the Health Checks that are to be performed on **EndPoints**.

To add Profiles, click on **Add Profiles** near the bottom of the window. This will provide you with an interface in which you can choose profiles from a number of different types. Choose the type, and the profile, that you wish to add to the policy.

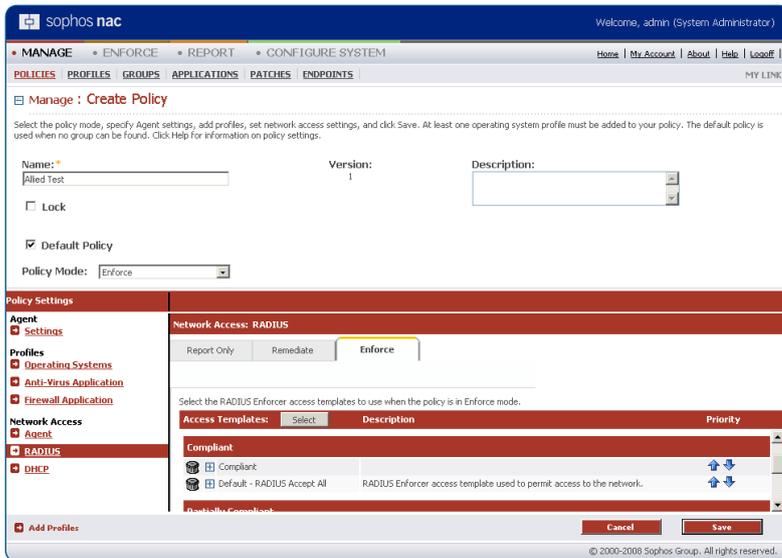
The illustration below shows an example of an anti-virus application profile being added.





As profiles are added, their types are added to a list at the lower left of the window, as shown below. The illustration below also shows how RADIUS Enforcer Access Templates are added to the policy.

Access Templates are added to each of the Compliant, Partially Compliant, and Non-Compliant sections of the Access Templates list. Multiple Templates can be added to each section, and are arranged in the order you wish a RADIUS request to be checked against them, until a template is found that matches the properties of that RADIUS request.



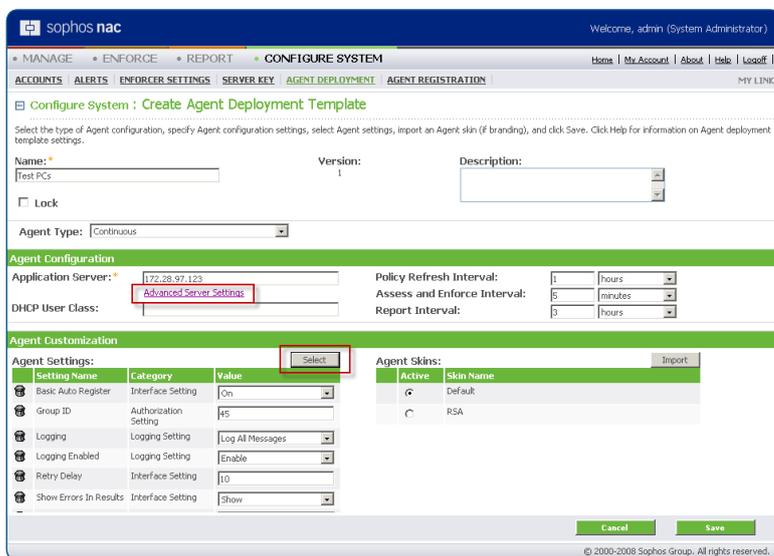
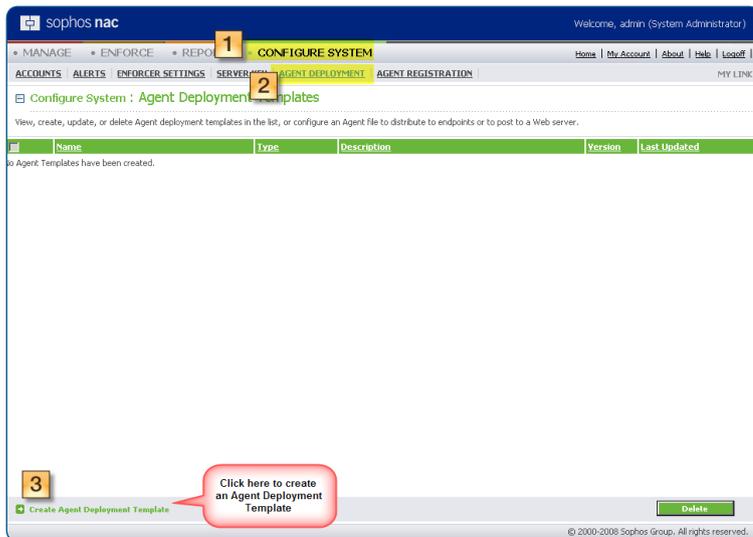
## Endpoint Agent deployment

The Application server creates the installer that installs the agent software onto endpoint devices.

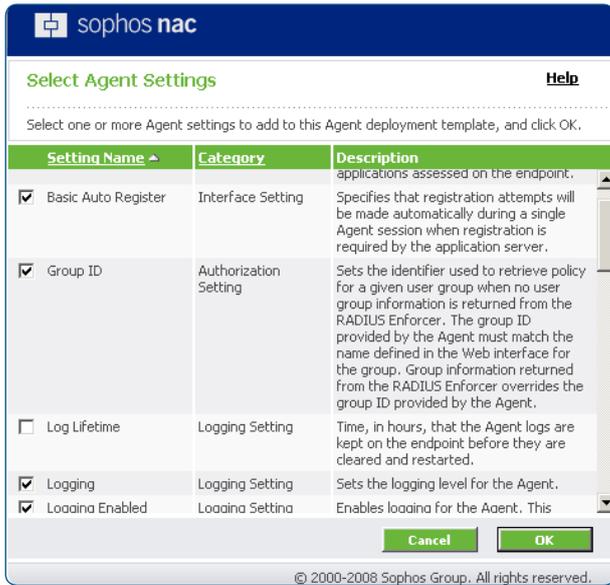
First an Agent Deployment Template is created, and then the installer is created, using settings defined in the Deployment Template.

### To create an Agent Deployment Template:

1. Select **Configure System**.
2. Select **Agent Deployment**, and you will be presented with the Agent Deployment Template interface.
3. Click **Create Agent Deployment Template** near the bottom of the window. This takes you to an interface for defining the details of the Agent Deployment Template.



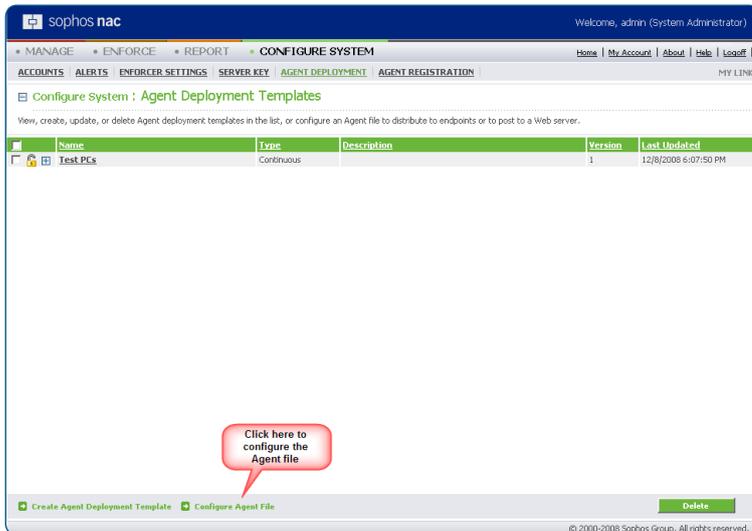
A number of quite detailed options can be configured, to control how the agent will operate, by clicking the **Select** button opposite **Agent Settings**.



Also, the **Advanced Server Settings** link gives you the opportunity to set some parameters on how the agent interacts with the server: In particular, you can choose whether the communication between agent and server is performed by HTTP or HTTPS. The communication defaults to HTTPS, but if you have any problem with HTTPS communication between the agent and the server, then choose the option of HTTP instead.

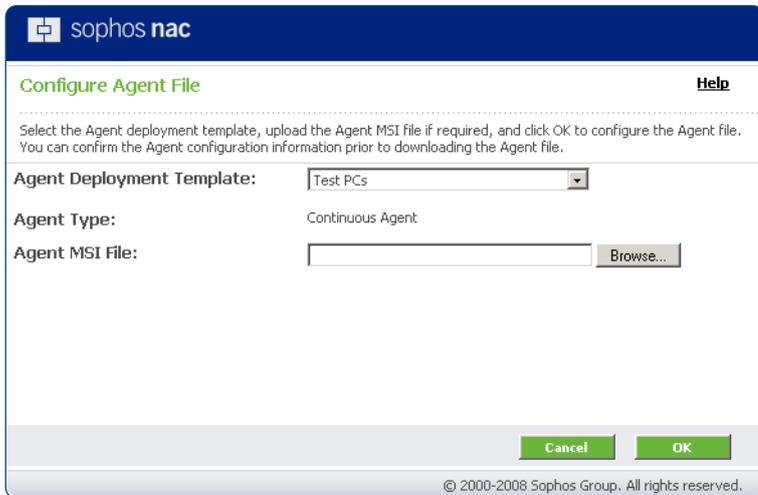
Once you have configured the desired settings on the Agent Deployment Template, you are ready to create the agent installation file.

Once a template has been created, the main Agent Deployment window will contain, near the bottom, a link labelled **Configure Agent File**.

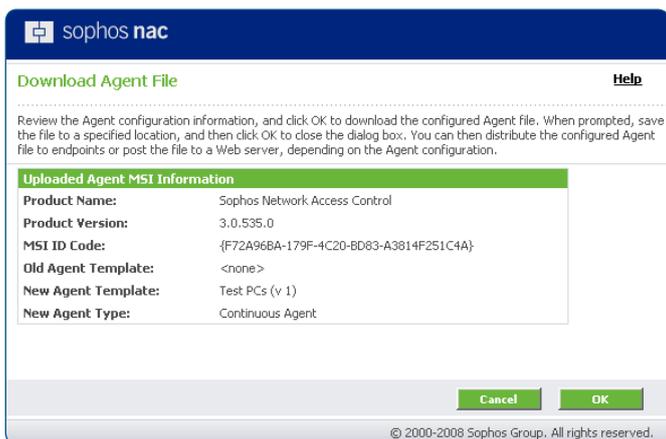


This link pops up a window that enabled you to configure the agent file.

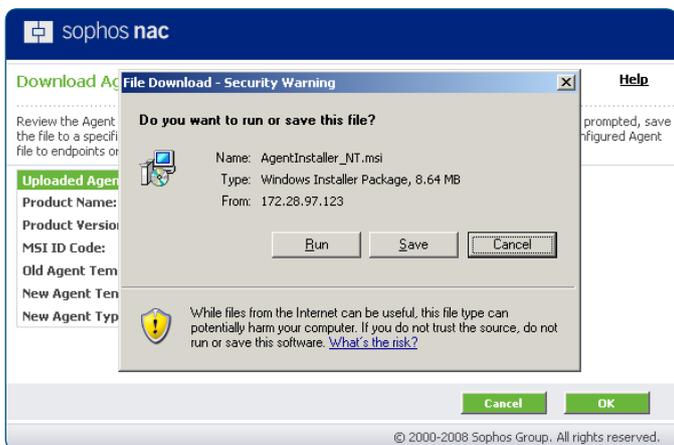
- Click **Browse...** to select and upload the initial Agent MSI file from which you want to create the new Agent file. You can obtain the default Agent MSI file from the Sophos Network Access Control installation CD.

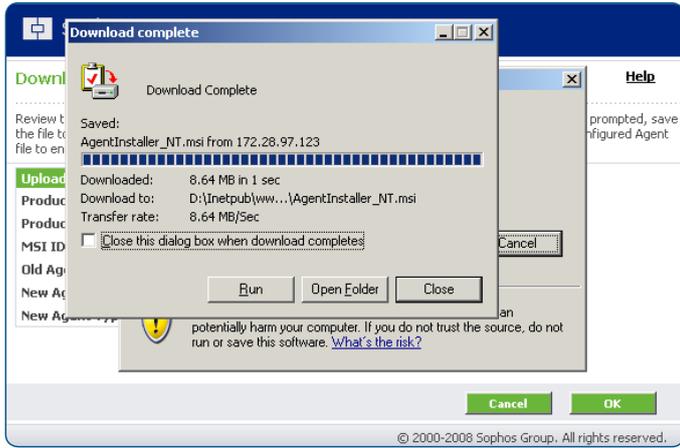


- Click **OK** in this window, and you will be provided with a summary of the details of the Agent msi file that's about to be created.



- Click **OK**, and the server will compile the Agent msi file, and give you the option to save it somewhere on the server.





## Deploying the Endpoint agent

To install the Sophos NAC Advanced agent onto an endpoint PC, copy the Agent .msi file (created above) onto the PC, and run it on the PC.

## Allied Telesis Switch configuration





## About Allied Telesis Inc.

Allied Telesis is a world class leader in delivering IP/Ethernet network solutions to the global market place. We create innovative, standards-based IP networks that seamlessly connect you with voice, video and data services.

Enterprise customers can build complete end-to-end networking solutions through a single vendor, with core to edge technologies ranging from powerful 10 Gigabit Layer 3 switches right through to media converters.

Allied Telesis also offer a wide range of access, aggregation and backbone solutions for Service Providers. Our products range from industry leading media gateways which allow voice, video and data services to be delivered to the home and business, right through to high-end chassis-based platforms providing significant network infrastructure.

Allied Telesis' flexible service and support programs are tailored to meet a wide range of needs, and are designed to protect your Allied Telesis investment well into the future.

Visit us online at [www.alliedtelesis.com](http://www.alliedtelesis.com)

---

USA Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895  
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11  
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830

[www.alliedtelesis.com](http://www.alliedtelesis.com)

© 2008 Allied Telesis Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners. C618-31017-00 RevA