

# **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 ||
- 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:

I. Run dcpromo.exe.

Run	<u>? ×</u>
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	dcpromo
	OK Cancel Browse

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

Active Directory Installation Wizard		
Domain Controller Type Specify the role you want this server to have.		
Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?		
Domain controller for a new domain		
Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.		
C Additional domain controller for an existing domain		
⚠️ Proceeding with this option will delete all local accounts on this server.		
All cryptographic keys will be deleted and should be exported before continuing.		
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.		
< <u>B</u> ack Next > Cancel		

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

reate	e New Domain
Se	elect which type of domain to create.
Cre	sate a new:
	Domain in a new forest
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.	
C Child domain in an existing domain tree	
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.	
O Domain tree in an existing forest	
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.	
	< Back Next > Cancel

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

Active Directory Installation Wizard	×
New Domain Name Specify a name for the new domain.	Se la companya de la
Type the full DNS name for the new domain (for example: headquarters.example.microsoft.cor	n).
Eull DNS name for new domain:	
Sophos-NAC.test.nz	
,	
	<u>B</u> ack <u>N</u> ext > Cancel

#### 5. Select Permissions as required.



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

Active Directory Installation Wiz	zard	×
Directory Services Restore This password is used when Mode.	Mode Administrator Password you start the computer in Directory Services Restore	R
Type and confirm the passwo when this server is started in f	rd you want to assign to the Administrator account used Directory Services Restore Mode.	
The restore mode Administrate account. The passwords for t both.	or account is different from the domain Administrator the accounts might be different, so be sure to remember	
Restore Mode Password:		
Confirm password:		
For more information about Di	irectory Services Restore Mode, see <u>Active Directory Help</u> .	
	< <u>B</u> ack <u>N</u> ext > Cance	

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**

I. Select Administrative Tools > Active Directory Domains and Trusts.

	Tusts Active Directory Domains and Trusts
	Active Directory Sites and Services Manages the trust relationships between domains.
😥 My Computer	📴 Certification Authority
	💼 Cluster Administrator
🐶 Control Panel	🖕 🤣 Component Services
	📃 Computer Management
Ministrative Tools	🖞 🏐 Configure Your Server Wizard
Rinters and Faxes	🗃 Data Sources (ODBC)
~	_ 🤰 Distributed File System
🕐 Help and Support	🚊 DNS
	🚡 Domain Controller Security Policy
>>> Search	🖗 Domain Security Policy

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.

Raise Domain Functional Level	×
Domain name:	
Sophos-NAC.test.nz	
Current domain functional level:	
Windows 2000 mixed	
Select an available domain functional level:	
Windows 2000 native	•
Windows 2000 native	
Windows Server 2003 on domain functional levels, click Help.	
<u>R</u> aise Cancel <u>H</u> elp	

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

## Creating the NAC service user account

#### I. Select Administrative Tools > Active Directory Users and Computers.

ve Programs		_
	Mattive Directory Sites and Services	Sort by: Name
	🍜 Active Directory Users and Computers	2010 071 IName
😏 My Computer	<ul> <li>Certification Authority</li> <li>Manages users, computers, se</li> <li>Cluster Administration the Active Directory.</li> </ul>	ecurity groups and other objects
📴 Control Panel 🛛 🔹	Component Services	Remo
Munistrative Tools	Configure Your Server Wizard	
Printers and Faxes	Data Sources (ODBC) Distributed File System	
Help and Support	A DNS	and the standard dealers, and the

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.

w Ubject - User			
🔄 💽 Ureate in:	Sophos-NAU.test.nz/Users		
<b>-</b>			
<u>F</u> irst name:	NAC	Initials:	
Last name:	Admin		
East Hamo.			
Full n <u>a</u> me:	NAC Admin		
	,		
<u>U</u> ser logon name:			
NacAdmin	@Sophos-N	IAC test nz ▼	
1	1 Cooprior II		
User logon name (pre	<u>W</u> indows 2000):		
SOPHOS-NAC\	NacAdmin		
1			
	< Back	Next > Cancel	
			_

# **NETWORK SECURITY SOLUTIONS** | Network Access Control (NAC)

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 <u>m</u> ust change password at next logon	
User cannot change password      Password never expires      Account is disabled	
< <u>B</u> ack <u>N</u> ext > 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.

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

💹 Microsoft SQL Server 2005 Setup	×
Installing Prerequisites Installs software components required prior to installing SQL	
Server.	
SQL Server Component Update will install the following components required for SQL Server Setup:	4
Microsoft SOL Native Client	
Microsoft SQL Native Client	
Click Install to continue.	
	<b>•</b>
[Irstall]	ncel

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

🔂 Microsoft SQL Server 2005 Express Edition Setup		
Feature Selection Select the program features you want installed.		
Click an icon in the following list to change how a feature	e is installed.	
Peature description     Database Services     Client Components     Connectivity Components     Software Development Kit     This feature requires 21 MB on your     hard drive.		
Installation path	Browse	
	Disk Cost	
Help < Back	Next > Cancel	

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

🖶 Microsoft SQL Server 2005 Exp	press Edition Setu	ıp	×
Authentication Mode The authentication mode specific connecting to SQL Server.	es the security used	when	
Select the authentication mode t	o use for this install	ation.	
☞ Windows Authentication Mod Mixed Mode (Windows Authentication)	dej entication and SQL S	erver Authentication	)
Specify the sa logon password b	elow:		
Confirm <u>p</u> assword:			
Help	< <u>B</u> ack	Next >	Cancel

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

🙀 Microsoft SQL Server 2005 Expr	ess Edition Setup	×
Ready to Install Setup is ready to begin installation	1.	
Setup has enough information to st change any of your installation set	art copying the program files. To pro tings, click Back. To exit setup, click C	iceed, click Install. To Cancel.
<ul> <li>The following component</li> <li>SQL Server Database (Database Services)</li> <li>Client Components (Connectivity Components)</li> </ul>	s will be installed: se Services	
Help	< <u>B</u> ack <u>I</u> nstall	Cancel

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.

🙀 Microsoft WSE 3.0 -	InstallShield Wizard	×		
Setup Type Choose the setup type that best suits your needs.				
Please select a setup	) type:			
• Runtime	Installs the runtime files only.			
C <u>A</u> dministrator	Runtime install plus standalone tools. Suitable for a deployment scenario where the tools are needed for configuration.			
O <u>D</u> eveloper	Adminstrator install plus documentation and samples. Microsoft .NET Framework SDK 2.0 or Microsoft Visual Studio 2005 are required to view the documentation. Microsoft Visual Studio 2005 is required to build and run the samples.			
C <u>V</u> isual Studio Developer	Developer install plus Visual Studio Tools. Microsoft Visual Studio 2005 is required for this installation type.			
C Cu <u>s</u> tom	Choose which program features you want installed and where they will be installed. Recommended for advanced users.			
InstallShield				
	< <u>B</u> ack <u>N</u> ext > Cancel			

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

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

#### I. Select Administrative Tools > IIS Manager.

😡 My Computer		Computer Management
<u> </u>	۲	Configure Your Server Wizard
🐶 Control Panel 🔹 🕨	7	Data Sources (ODBC)
	Ŀ	Distributed File System
Administrative Tools	2	DNS
😂 Printers and Faxes	6	Domain Controller Security Policy
	6	Domain Security Policy
Help and Support	9	Event Viewer
C caunt		Internet Authentication Service
	۱	Internet Information Services (IIS) Manager
70 <u>R</u> un	C:	Licensing
	3	Manage Your Server
	<u> -</u>	Microsoft .NET Framework 1.1 Configuration
	<u>e</u>	Microsoft .NET Framework 1.1 Wizards

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.

#### I. 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.

🦻 Internet Authentication Service			_ 🗆 🗙	
Eile Action View Help				
P Internet Authentication Service (Local)	Name	0	rder	
RADIOS Clients     Remote Access Longing	There ar	e no items to show in this view.		
- W Remote Access Policies				
Connection Request Prc     New Remote Access F	olicy			
New	•			
View	•			
Refresh				
Export List				NT REGISTRATION
Halp				
<u> </u>				
				port an Agent ckin (if branding)
				ipore an egone skir (ir branding)
U and a second	U maada saa aha	and the second s		have a second and a second

4. Select Set up a custom policy, and give it a name like Dot Ix Users.

New Remote Acce	ss Policy Wizard
Policy Configu The wizard c	ration Method an create a typical policy, or you can create a custom policy.
How do you w	vant to set up this policy?
◯ <u>U</u> se the	e wizard to set up a typical policy for a common scenario
	a custom policy
Type a name t	hat describes this policy.
Folicy name.	Dot'ix Users
	Example: Authenticate all VPN connections.
	< <u>B</u> ack <u>N</u> ext > Cancel

5. Choose to Add a policy condition.

New Remote Access Policy Wizard	×
Policy Conditions To be authenticated, connection requests must match the conditions you specify.	
Specify the conditions that connection requests must match to be granted or denied access.	
Add Edit Remove	
< <u>B</u> ack <u>N</u> ext > Cancel	

6. Select the attribute NAS-Port-Type.



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

NAS-Port-Type		<u>?</u> ×
Available types: ADSL-CAP - Asymmetri ADSL-DMT - Asymmetri Async (Modem) Cable FDDI G.3 Fax HDLC Clear Channel IDSL - ISDN Digital Su ISDN Async V.120 ISDN Sync V.120	<u>Add</u> >> Ethernet	•
	OK Can	cel

#### 8. Click OK.

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

New Remote Access Policy Wizard	×
Permissions A remote access policy can either grant or deny access to users who match the specified conditions.	ŷ
If a connection request matches the specified conditions:	
Deny remote access permission     Grant remote access permission	
,	
< <u>B</u> ack <u>N</u> ext >	Cancel

#### 9. Click Next.

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

#### IO. Click Edit Profile...

New Remote Access Policy Wizard	×
Profile You can make changes to the profile for this policy.	Ŷ
A profile is a collection of settings applied to connection requests that have been authenticated. To review or change the default profile for this policy, click Edit Profile.	
Edit Profile	
< <u>B</u> ack ( <u>Next&gt;</u> ) Can	cel

## **NETWORK SECURITY SOLUTIONS** | Network Access Control (NAC)

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.

Dial-in Profile	_		? ×	
Dial-in Constraints	IP IP	Multilink		
Authentication	Encryption	Advanced		
EAP Methods  Microsoft Encrypted Au  Microsoft Encrypted Au  Uger can chang  Encrypted authenticati Unauthenticated accomments  Alter center to accomments	thentication version 2 (f e password after it has e thentication (MS-CHAP e password after it has e on (CHAP) ation (PAP, SPAP)	AS-CHAP v2) xpired Select EAP Pr EAP (ypes are	Add EAP Authentication methods: Smat Card or other certificate	<u> 1</u> ×
method.	Control of the second starting and	EAP (ypes:	MD5-Challenge	Move Up
				dave Dav
	OK Ca			MOVEIDON
		<u>A</u> dd	ОК С	ancel Cancel

#### 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.

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

🐤 Internet Authenti	cation Service		
<u>File Action V</u> iew	Help		1
	1 0 🖻 😫	E	
🕺 Internet Authentica	tion Service (Local)		Friendly Name
RADIUS Clients     Remote Access	New RADIUS <u>C</u> lie	ent	.U.EFServer
E Remote Access	<u>N</u> ew	•	
	⊻iew	•	
	Refresh		
	Export <u>L</u> ist		· · · ·
	Help		
	بالأسعاد والمحمد والمحمد		

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

New RADIUS Client		×
Name and Address		
Type a friendly name and either a	n IP Address or DNS name for the client.	
Eriendly name:	×600	
Client address (IP or DNS):		
172.28.68.56	[]	
	< Back Next > Cancel	

New RADIUS Client		×
Additional Information		
If you are using remote access po vendor of the RADIUS client.	olicies based on the client vendor attribute, specify the	
<u>C</u> lient-Vendor:		
RADIUS Standard		
<u>S</u> hared secret:	мининини	
C <u>o</u> nfirm shared secret:	MINIMUM	
<u>R</u> equest must contain the M	fessage Authenticator attribute	
	< <u>B</u> ack Finish Cancel	

## **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.

Internet Authentication Service		1
<u>File Action View H</u> elp		
← → 🗈 🖬 🖻 🗟 😭 🖬		
Internet Authentication Service (Local)     ADJUS Clients     Remote Access Logging     Remote Access Policies     Connection Request Processing	Start Service Stop Service Register Server in Active Directory Properties Help	

### 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:

- **I.** 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.

Console1 - [Console Roo       Pie         G       Ele       Action       View       Par         ←       →       Ele       Ele       Ele       Ele         Console Root       Name	t] vgrites Window Help Add/Remove Snap-in Standalone Extensions Use this page to add or remove a stand-alone	snap-in from the console.	
	Snap-ins added to: 🔄 Console Root	Add Standalone Snap-in	<u>? ×</u>
		Available standalone span-inst	
		Spap-in	Vendor
		MET Eramework 1.1 Configuration	Microsoft Corporation
		Active Directory Domains and Trusts	Microsoft Corporation
		Active Directory Sites and Services	Microsoft Corporation
		Active Directory Users and Compu	Microsoft Corporation
		a ActiveX Control	Microsoft Corporation
		Authorization Manager	Microsoft Corporation
		Certificate Templates	Microsoft Corporation
	Description	Certificates	Microsoft Corporation
	Description	E Certification Authority	Microsoft Corporation
		Component Services	Microsoft Corporation
	Add <u>R</u> emove About.	─Description The Certificates snap-in allows you to bro certificate stores for yourself, a service,	wese the contents of the or a computer.
			Add <u>C</u> lose

- 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).

🚡 Console1 - [Console Root\Certificates (Local Compute	r)]					
🚡 Eile Action View Favorites Window Help						
Console Root Logical Store Name						
Certificates (Lo Trusted Root Certification Authoritie	Find Certificates					
Enterprise Trust	All Tas <u>k</u> s 🔸	Find Certificates				
	New Window from Here	Request New Certificate				
Untrusted Certificates	Refresh -	Import				
Trusted People	Help					
Certificate Enrollment Requests		·				
Request a new certificate from a certification authority (CA) in your	r domain					

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.

🐌 Internet Information Serv	vices (IIS) Manager				
🐚 Eile Action View Window Help					
← → 🗈 💽 🗙 😭	3 🗈   🔮 💷   💂   ▶ ■ 🗉 👌				
Internet Information Services  TEST-6MU4D9283T (local  FTP Sites  Web Sites  Web Sites  Web Sites  Default Settered  Default Web Sites  Default Settered  Default Web Sites  Default We	s Name I computer) MSMQ WebAgent isstart.htm Explore pror.gif				
B WED BEFYILE EXCELSI	Open Permissions Browse				
	Stop Pause				
	New				
	View ► New Window from Here				
	Delete Rename Refresh				
Opens the properties dialog box f	Export List				
	Нер				
- A second a second data da a seconda a seconda da a second	المريبية بمسمور متصر وكلاه فمالقصف				

#### 6. Click Server Certificate.



#### 7. Select Assign an existing certificate.

IIS Certificate Wizard 🛛 🔀
Server Certificate These are the methods for assigning a certificate to a Web site.
Select the method you want to use for this web site:
< <u>B</u> ack <u>N</u> ext > Cancel

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.

IIS Certificate Wizard							
Available Certificates The certificates you can use for your Web server are listed below.							
Select a certificate							
Issued To	Issued By	Expiration Date	Intended Purpose F				
test-6mu4d9z83	St Root CA	11/18/2009	Client Authentic				
test-6mu4d9z83	3t Root CA	12/4/2009	Client Authentic				
Hoot LA	Hoot LA	11/18/2013					
		< <u>B</u> ack	Next > Cancel				

# NETWORK SECURITY SOLUTIONS | Network Access Control (NAC)

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

IIS Certificate Wizard	×
SSL Port Specify the SSL port for this web site.	
SSL port this web site should use:	
	< <u>B</u> ack Next> Cancel

#### 9. Click Next.

**IO.** 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.

🙀 Sophos NAC Databa	ses - InstallShield Wizard	×
<b>SQL Server Informa</b> Select the SQL Serve	tion r instance and the authentication method for installation.	2
SQL Server: Connect Using:	.\SQLEXPRESS	
Login Name: Password:		
InstallShield	< <u>B</u> ack <u>N</u> ext > Cancel	

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.

🕞 Sophos NAC Databases - InstallSh	nield Wizard 🔀			
SQL Server Information This information allows the appropriate accounts to be created in SQL Server.				
Sophos NAC Service Account (Domain\Username) Service Account Password	Sophos-NAC'(NacAdmin			
Verify Password	*****			
InstaliShield	< Back Next > Cancel			

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.

🔂 Sophos NAC Application Server - In	×			
Sophos NAC Specify the required information to complete the installation.				
SQL Server Instance I	Vame	,\SQLE>	press	
Service Account (Domain\User	name)	Sophos	-NAC\NacAdmin	
Service Account Pass	word	*****	***	
Verify Pass	word	*****	***	
Registration Interface's RADIUS Shared S	Secret	*****	***	
Verify RADIUS Shared Secret ********				
Select the root folder for the II: D:\Inetpub\www.wroot\ InstallShield	5 applicati	ons.		Change
	< <u>B</u>	ack	<u>N</u> ext >	Cancel

# NETWORK SECURITY SOLUTIONS | Network Access Control (NAC)

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:

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

<b>b</b> sophos <b>nac</b>	
Welcome to Sophos NAC : Login	
Assessment Blances*	}
Admin	
Password:*	
*required	Login
Supported Microsoft® Browsers	1

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.

Welcome to Sophos NAC:Login
i You must specify a new password for this account.
Account Name:*
admin
Password:* Confirm New Password:*
••••••     Login     *required
Supported Microsoft® Browsers
Internet Evoluter 6-0

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

I. 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.

ophos nac		Welcome, Admin (System Administrator)
MANA     MANA     MANA     MANA     MANA	REPORT     CONFIGURE SYSTEM	Home   My Account   About   Help.   Logoff
AGENT ENFORCER ACCESS TEMPLA	2 RADIUS ENFORCER ACCESS TEMPLATES DHCP ENFORCER ACCESS TEMPLATES NETWO	ORK RESOURCES EXEMPTIONS MY LINKS
E Enforce : RADTUS Enfo	rcer Access Templates	
view, create, update, or delete RADIU:	Enrorcer access templates in the list.	
Name Name	Description	Version Last Updated
🗆 🔓 🖃 Default - RADIUS Accep	All RADIUS Enforcer access template used to permit access to the network.	1 12/1/2008 4:27:21 PM
RADIUS Enforcer Acces	s Template Details	
Name:	Default - RADIUS Accept All	
Version:	1 Participation of the second se	
Compliance States:	RADIUS Enforcer access template used to permit access to the network.	
Network Access:	accept	
RADIUS Client IP Addr	sses: RADIUS Attributes:	
IP Address	Name Number Type Vendor Code Vendo	or Sub Value
Any	No Attributes	
🗖 🔓 📃 Default - RADIUS Reject	All RADIUS Enforcer access template used to deny access to the network.	1 12/1/2008 4:27:22 PM
RADIUS Enforcer Acces	s Template Details	
Name:	Default - RADIUS Reject All	
Version:	1	
Description:	RADIUS Enforcer access template used to deny access to the network.	
Compliance States:		
RADIUS Client IP Addr	sses: RADIUS Attributes:	
IP Address	Name Number Type Vendor Code Vendo	or Sub Value
Any	Click here to add	bute
2	new Access	
	l emplates	Delate
Create RADIOS Enforcer Access 1	mprace	Delete
L		© 2000-2008 Sophos Group, All rights reserved,

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

🖕 sophos <b>nac</b>					Welcom	e, admin (System Admin	istrator)	
MANAGE     • ENFORCE     • RE	EPORT •	CONFIGURE SYSTE	M		Home   (	My Account   About   Help	Logoff	
AGENT ENFORCER ACCESS TEMPLATES	ADIUS ENFOR	CER ACCESS TEMPLATES	DHCP ENFORCER A	CCESS TEMPLATES	NETWORK RESOU	RCES EXEMPTIONS	MY LINKS	
Enforce : Create RADIUS Enforcer Access Template								
Select the template compliance states, add RADIUS client IP addresses or select ANV, specify Accept or Reject network access, create associated RADIUS attributes, and click Save. Click Help for information on access template settings.								
Name:*	Version:	Description:		Template Compli	iance States:	🔮 🗹 Compliant		
Compliant	1		*	(Obda Whiten choacing)	policy)	Partially Compliant     Non-Compliant		
Lock						<ul> <li>Enter compidit</li> </ul>		
RADIUS Client IP Addresses		RADIUS Attrib	utes					
ANY 0.0.0.0	Add	Network Acc	ess: Accept	•			_	
		Attributes	New	Properties	La de la			
		Tunnel-type		Type:	Standard	•	-	
		-		Name:*	Tur	nnel-type		
				Number:*	64			
				Format: Value:*	13	eger 💌		
					1			
				-				
						_		
					Cancel	Save		
					© 2000-20	08 Sophos Group. All rights	reserved.	

- 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

# NETWORK SECURITY SOLUTIONS | Network Access Control (NAC)

ophos nac					Welcom	e, admin (System Adminis	strator)
• MANAGE • ENFORCE • F	EPORT • CO	FIGURE SYSTEM			Home	My Account   About   Help	Logoff
AGENT ENFORCER ACCESS TEMPLATES	RADIUS ENFORCER A	CESS TEMPLATES	ENFORCER ACC	ESS TEMPLATES	NETWORK RESOL	RCES EXEMPTIONS	MY LINKS
Enforce : Create RADIUS E	nforcer Access	Template					
Select the template compliance states, add RA information on access template settings.	DIUS client IP addresse	or select ANV, specify Accep	t or Reject networ	k access, create ass	ociated RADIUS attr	ibutes, and click Save. Click H	telp for
Name:* Compliant	Version: Des 1	cription:	*	Template Comp (Used when creatin	pliance States: g policy)	Compliant	
Lock			<b>v</b>			🖉 🗖 Non-Compliant	
RADIUS Client IP Addresses		RADIUS Attributes					
Many Daga	Add	Network Access:	Accept				
10.0.0.0	100	Attributes	New	Properties			
		Tonel-Medium-Typ	e _	Type:	Standard	×	
		m runner-type		Name:*	To	nel-Medium-Type	
	¥	1		Number:*	65		
				Format:	In	eger 🔽	
				Value:*	6		
				-1			
		-					
ophos nac					Welcon	ne, admin (System Admin	istrator)
• MANAGE • ENFORCE • F	REPORT • CO	NFIGURE SYSTEM			Home	<u>My Account</u>   About   Help	Logoff
AGENT ENFORCER ACCESS TEMPLATES	RADIUS ENFORCER A	CCESS TEMPLATES DHC	PENFORCER ACC	ESS TEMPLATES	NETWORK RESOL	IRCES EXEMPTIONS	MY LINK
Enforce : Create RADIUS E	inforcer Access	Template					
Select the template compliance states, add R/ information on access template settings.	DIUS client IP addresse	s or select ANY, specify Accep	it or Reject netwo	rk access, create as	sociated RADIUS att	ributes, and dick Save. Click I	Help for
Name:*	Version: Des	cription:		Template Com	pliance States:	🍼 🗹 Compliant	
Compliant				(used micrococi	ig posesy	Partially Compliant	
Lock						<ul> <li>Non-complianc</li> </ul>	
RADIUS Client IP Addresses		RADIUS Attributes					
₩ ANY 0.0.0.0	Add	Network Access:	Accept				-
	×	Attributes	New	Properties			
		Trinel-Medium-Type	um.	Type:	Standard	•	
		Tunnel-type		Name:*	Tu	nnel-Private-Group-ID	
	<u> </u>	1		Number:*	81		
				Format:	T	• txe	
				Value:*	10		
				-1			

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 dropdown menu.

		Welcome, admin (System Administrator)
REPORT	CONFIGURE SYSTEM	Home   My Account   About   Help   Logoff
APPLICATIONS	PATCHES ENDPOINTS	MY LINKS
the list.		
	User Groups	Version Last Updated
	• REPORT	REPORT     CONFIGURE SYSTEM      PAICHES     ENDPOINTS      the lat.      User Groups

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

¢	SO	phos nac			Welcome, adn	nin (Syste
• MAN	NAG	E • ENFORCE • REPORT •	CONFIGURE SYSTEM		Home   My Acc	ount   Ab
POLICI	IES	PROFILES GROUPS APPLICATIONS PA	TCHES ENDPOINTS			
E Ma	anad	ae : Profiles				
Search	for, s	view, create, update, or delete profiles in the list.				Ì
Searc	ch Cr	iteria				
				1		
Nar	ne:		Type: All			
	Disp	olay Profiles Added in the Last 7 Days.	Reset	Search		
		Profiles <del>-</del>	Туре	Profile Item	Version	Last!
	Ŧ	WinXP Profile	Operating System	Windows XP	1	12/1/2
	Ŧ	WinVista Profile	Operating System	Windows Vista	1	12/1/2
	+	Windows Live OneCare 1.x Profile	Anti-Virus Application	Windows Live OneCare 1.x	1	12/8/2
🗆 🔓	Ŧ	Windows Defender 1.x Profile	Anti-Spyware Application	Windows Defender 1.×	1	12/8/2
	Ŧ	Win985E Profile	Operating System	Windows 98 SE	1	12/1/2
	+	Win2K Profile	Operating System	Windows 2000	1	12/1/2
	+	Win2003 Profile	Operating System	Windows 2003	1	12/1/2
	Ħ	Trend Micro OfficeScan Corporate Edition 7.x Profi	Anti-Virus Application	Trend Micro OfficeScan Corporate Edition 7.x	1	12/8/2
	Ŧ	Trend Micro OfficeScan Client 7.x Profile	Anti-Virus Application	Trend Micro OfficeScan Client 7.x	2	12/8/2
	Ŧ	Trend Micro OfficeScan Client 7.x Profile	Firewall Application	Trend Micro OfficeScan Client 7.x	1	12/8/2
	+	Trend Micro Anti-Spyware 3.x Profile	Anti-Spyware Application	Trend Micro Anti-Spyware 3.x	1	12/8/2
	Ŧ	Symantec Client Security 10.x Profile	Firewall Application	Symantec Client Security 10.×	1	12/8/2
	Ŧ	Symantec AntiVirus 10.x Profile	Anti-Virus Application	Symantec AntiVirus 10.×	2	12/8/2

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.

🖕 sophos <b>nac</b>		Welcome, admin	(System Administrator)					
MANAGE     ENFORCE     REPORT	CONFIGURE SYSTEM	Home   My Accou	nt   <u>About</u>   <u>Help</u>   <u>Logoff</u>					
POLICIES PROFILES GROUPS APPLICATIONS P	PATCHES ENDPOINTS		MY LINKS					
Manage : Update Profile	🖻 Manage : Update Profile							
Select the profile item; specify the Installed/Else compliance st actions; and click Save. Click Help for information on profile set	ates and messages; add service packs, patches, or c things.	apabilities to the profile; specify the associated condit	ions, compliance states, and					
Name: * Microsoft Windows Firewall XP SP2 Profile *nguited - Lock	Version: 1	Description: Microsoft Windows Firewall XP SP2 Profile	* *					
Application: Microsoft Windows Firewall XP SP	Application: Microsoft Windows Firewall XP SP2 Operating Systems: 👿 Agent Types: 🏰 🛃							
Condition Compliance Stat	te Message							
Installed Compliant	▼ No Message ▼							
Else Non-Compliant	🗴 Show Message 💽 🤅							
Application Capabilities								
😭 Enabled	Operating Systems: 😠	Agent Types: 🔩	<b>2</b>					
Condition	Compliance State Message	Remediation Actions	Prioritize					
Enabled 🔽	Compliant No Message	Enable						
Else	Non-Compliant Show Message	💽 😼 🔽 Enable						
View Usage Details		Cancel Save As New	Save					

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.

ophos nac		Velcome, admin	(System Administrator)
MANAGE      • ENFORCE      • REPORT      • CONFIG	GURE SYSTEM	tome   <u>My Accou</u>	nt   Albout   Help:   Logoff
POLICIES PROFILES GROUPS APPLICATIONS PATCHES E	NDPOINTS		MY LINKS
Manage: Policies			
View, create, update, or delete policies in the list.			
Policies I	User Groups Yer	sion La	ast Updated
o policies have been created.			
Click here to create a new			
Policy			
Create Policy			Delete
~	0	2000-2008 Sopho	s Group. All rights reserved.

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.

📮 sophos nac		Welcome, admin (System Administrator)
MANAGE     ENFORCE	REPORT     CONFIGURE SYSTEM	Home   <u>My Account</u>   <u>About</u>   <u>Help</u>   <u>Logoff</u>
POLICIES PROFILES GROUPS	APPLICATIONS PATCHES ENDPOINTS	MY LINKS
Manage : Create Policy		
Select the policy mode, specify Agent se used when no group can be found. Click	ttings, add profiles, set network access settings, and click Save. At least one Help for information on policy settings.	e operating system profile must be added to your policy. The default policy is
Name:*	Version:	Description:
Alied Test	1	<u>~</u>
Lock		×
Default Policy     Policy Mode: Enforce		
Policy Settings		
Agent Settings	Agent Settings	
Profiles	Continuous Agent Settings	Quarantine Agent Settings
🖸 Operating Systems 📩	Policy Pefreth Interval	Quarantina Oversider
Network Access	This value identifies how often the Continuous or	This value identifies whether endpoint users can override
RADIUS	Quarantine Agent retrieves policy.	quarantine.
DHCP	Assess and Enforce Interval: 5 Minutes	DHCP Agent Settings
	This value identifies how often the Continuous or Quarantine Agent verifies if the endpoint is in	Agent Enforcement Action: None
	comprance.	This value establishes the method used to obtain new IP addresses for the endpoint.
Click	here to add as have often the Continuous or	
D Add Profiles	Totiles	Cancel Save
-		© 2000-2008 Sophos Group, All rights reserved.

# NETWORK SECURITY SOLUTIONS | Network Access Control (NAC)

¢	sophos <b>nac</b>							
Selec	t Profiles	Help						
Select t adding Profile	Select the profile type and associated profiles to add to the policy, and click OK. At least one operating system profile must be added to your policy prior to adding other profiles. Profile Type: Anti-Virus Application •							
🛢 Sea	rch							
Name:	Operating System:	All Operating Systems						
		Reset						
	Profiles -	Description						
□ 🗄	CA eTrust Antivirus 7.x Profile	CA eTrust Antivirus 7.x Profile						
□ ⊞	McAfee VirusScan Enterprise 8.0.0.× Profile	McAfee VirusScan Enterprise 8.0.0.x Profile						
□ 🗄	Sophos Anti-Virus 4.6 Profile	Sophos Anti-Virus 4.6						
□ ⊞	Sophos Anti-Virus 6.× Profile	Sophos Anti-Virus 6.x Profile						
▼ 🗄	Sophos Anti-Virus 7.x Profile	Sophos Anti-Virus 7.x Profile						
□ ⊞	Symantec AntiVirus 10.× Profile	Symantec AntiVirus 10.× Profile						
□ ⊞	Trend Micro OfficeScan Client 7.x Profile	Trend Micro OfficeScan Client 7.x Profile						
□ ⊞	Trend Micro OfficeScan Corporate Edition 7.× Profile	Trend Micro OfficeScan Corporate Edition 7.× Profile						
□ ⊞	Windows Live OneCare 1.x Profile	Windows Live OneCare 1.x Profile						
		- 						
		Cancel						
		© 2000-2008 Sophos Group. All rights reserved.						

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.

p sophos nac				Weld	come, admin (System Administrator)
MANAGE         • ENFORCE	e • REPORT	CONFIGURE SYSTE	м	Hom	e   <u>Mv.Account</u>   <u>About</u>   <u>Helo</u>   <u>Logoff</u>
POLICIES PROFILES GROUP	APPLICATIONS	PATCHES ENDPOINTS			MY LINKS
Manage : Create Pol	icy				
Select the policy mode, specify Age used when no group can be found.	nt settings, add profile Click Help for informatio	, set network access settings, and n on policy settings.	l click Save. At least on	e operating system profile must be add	ed to your policy. The default policy is
Name:*		Version:		Description:	
Allied Test		1			~
□ Lock					~
Default Policy					
Policy Mode: Enforce	•				
Policy Settings					
Agent Settings	Network Acces	a: RADIUS			
Desfiles	Report Only	Remediate Enfo	arce		
Operating Systems			1		
Anti-Virus Application					
Firewall Application	Select the RADI	JS Enforcer access templates to us	e when the policy is in	Enforce mode.	
Network Access Access	Access Temp	lates: Select De	scription		Priority
RADIUS	Compliant				
DHCP	😭 🗄 Comp	iant			<b>≙ ∛</b>
	쮦 🗄 Defau	It - RADIUS Accept All RAI	DIUS Enforcer access to	emplate used to permit access to the ne	stwork. 🏠 😽
	Davitally Co	noliont			•
Add Profiles				C	ancel Save
				© 200	0-2008 Sophos Group, All rights reserved.

## **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:

#### I. 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.

🖕 sophos na	c					Welcome, a	dmin (System Admi	nistrator)
• MANAGE • EN	FORCE • REPO	CONFIG	URE SYSTEM	1		Home My a	Account   About   Hel	e   Logoff
ACCOUNTS ALERTS	ENFORCER SETTINGS	SERVER	T DEPLOYMENT	AGENT REGISTRA	ATION			MY LINKS
E Configure Syste	em : Agent Deplo	vmen 2 hpla	rtes					
View, create, update, or c	lelete Agent deployment te	emplates in the list, or co	onfigure an Agent	file to distribute to en	dpoints or to post to a '	Web server.		
= Name		Type	Descr	ption		Version	Last Undated	
Agent Templates have be	en created.	1000	<u>besch</u>	peron		TELSION	cuscopulicu	
			_					
3	(	Click here to cre	ate					
Create Agent Deploys	nent Template	an Agent Deployr Template	nent				Delete	
						@ 2000-2008 ·	iophos Group, All right	s reserved
						-		
🖕 sophos na	c					Welcon	ne, admin (System .	Administrator)
MANAGE         • E	NFORCE • REP	ORT • CONFI	GURE SYSTE	EM		Home	My Account   About	Help   Logoff
ACCOUNTS ALERTS	ENFORCER SETTINGS	SERVER KEY AG	ENT DEPLOYMEN	AGENT REGIS	TRATION			MY LI
🗉 Configure Syst	em : Create Age	nt Deploymen	t Template					
Select the type of Agent	configuration, specify Age	nt configuration setting	js, select Agent s	ettings, import an Ag	ent skin (if branding), a	and click Save. Click Hel	o for information on A	gent deploymer
template settings.								
Test PCs		7	Version:		Description:		*	
							-	
LOCK								
Agent Type: Conti	nuous	*						
Agent Configuration								
Application Server:	172.28.97.123			Policy Refresh	Interval:	1 hours	•	
DHCD Hoor Classy	Advanced Server	Settings		Assess and Er	force Interval:	5 minut	35 💌	
DHUP USER Class:				Report Interv	al:	3 hours	•	
Agent Customizatio	า	_						
Agent Settings:			Select	Agent Skins:			Import	
Setting Name Basic Auto Register	Category Interface Settion	Value	_	Active	Skin Name Default			
Group ID	Authorization	45		· ·	RSA			
	Setting	10		U				
Logging	Logging Setting	Log All Messages	-					
FINE CONTRACTOR CONTRACTOR	Logana Setting							
Retry Delay	Logging Setting	Enable						

•

Show

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

cel Save

8

Show Errors In Results Interface Setting

🖕 sophos <b>nac</b>							
s	Select Agent Settings Help						
Se	elect one or more Agent s	ettings to add to this	Agent deployment template, and click OK.				
	Setting Name 🔺	<u>Category</u>	Description				
_			applications assessed on the endpoint.				
V	Basic Auto Register	Interface Setting	Specifies that registration attempts will be made automatically during a single Agent session when registration is required by the application server.				
R	Group ID	Authorization Setting	Sets the identifier used to retrieve policy for a given user group when no user group information is returned from the RADIUS Enforcer. The group ID provided by the Agent must match the name defined in the Web interface for the group. Group information returned from the RADIUS Enforcer overrides the group ID provided by the Agent.				
	Log Lifetime	Logging Setting	Time, in hours, that the Agent logs are kept on the endpoint before they are cleared and restarted.				
$\checkmark$	Logging	Logging Setting	Sets the logging level for the Agent.				
$\mathbf{V}$	Logging Enabled	Loaaina Settina	Enables logging for the Agent. This				
			Cancel				

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**.

🖕 sophos nac			Welcome, ad	min (System Administrator)	
MANAGE     ENFORCE     REPORT	CONFIGURE S	YSTEM	Home   My Ac	count   <u>About</u>   <u>Helo</u>   <u>Logoff</u>	
ACCOUNTS ALERTS ENFORCER SETTINGS SERVER	KEY AGENT DEPLO	IYMENT AGENT REGISTRATION		MYLINKS	
E Configure System : Agent Deployment	t Templates				
View, create, update, or delete Agent deployment templates in the list, or configure an Agent file to distribute to endpoints or to post to a Web server.					
Name	Type	Description	Version	Last Updated	
🗆 🔓 🎛 Test PCs	Continuous		1	12/8/2008 6:07:50 PM	
Č	click here to onligure the Agent file				
Create Agent Deployment Template Deployment Template	nt File			Delete	
Create Agent Deployment Template Configure Age	nt File		@ 2020 2020 C-	Delete	

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.

🖕 sophos <b>nac</b>	
Configure Agent File	Help
Select the Agent deployment template, uplo You can confirm the Agent configuration info	ad the Agent MSI file if required, and click OK to configure the Agent file. ormation prior to downloading the Agent file.
Agent Deployment Template:	Test PCs
Agent Type:	Continuous Agent
Agent MSI File:	Browse
	Cancel OK
	© 2000-2008 Sophos Group. All rights reserved.

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.

🖕 sophos <b>nac</b>					
Download Agent File	Download Agent File				
Review the Agent configuration information, and click OK to download the configured Agent file. When prompted, save the file to a specified location, and then click OK to close the dialog box. You can then distribute the configured Agent file to endpoints or post the file to a Web server, depending on the Agent configuration.					
Uploaded Agent MSI Inform	ation				
Product Name:	Sophos Network Access Control				
Product Version:	3.0.535.0				
MSI ID Code:	{F72A96BA-179F-4C20-BD83-A3814F251C4A}				
Old Agent Template:	<none></none>				
New Agent Template:	Test PCs (v 1)				
New Agent Type:	Continuous Agent				
	Cancel	ОК			
	© 2000-2008 Sophos Group. All	rights reserved.			

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**

Sends authentication requests to the Network Policy Server at 192.168.0.2

Sets the switch to use the configured RADIUS servers for  $802.1 \times authentication$ 

Creates the DHCP pool for client PCs that the Network Policy Server deems noncompliant. These are allocated an IP address in the range 192.168.2.167 - 192.168.2.200

Creates the DHCP pool for client PCs that the Network Policy Server deems compliant. These PCs are allocated an IP address in the range 192.168.10.167 – 192.168.10.200

Enables the DHCP server

Creates the ACLs that will restrict network access to the client PCs. Compliant PCs (with an IP address in the 192.168.10.0 subnet) are allowed normal access to the network.

Noncompliant PCs (with an IP address in the 192.168.2.0 subnet) are allowed access ONLY to the servers.

Allows all DHCP traffic.

Sets the switch to drop all traffic that does not match the other  $\ensuremath{\mathsf{ACLs}}$ 

Creates the compliant and noncompliant VLANs. There are no statically allocated ports on these VLANs. Instead the switch dynamically allocates the ports using the 802.1X VLAN assignment process.

Sets ports 1.0.1-1.0.8 to be non-authenticating ports. Connect servers and routers to these ports.

Sets the remaining ports as authenticating ports. The ACLs that constrain the access to the network are applied to these ports.

 $802.1\,\mathrm{X}$  is enabled on these ports and configured to accept dynamic VLAN assignment.

Allocates IP addresses to all the VLANs on the switch, so that it can L3 switch between these VLANs.

radius-server host 192.168.0.2 key testing 123-2 aaa authentication dot I x default group radius ip dhcp pool NAC-noncompliant network 192.168.2.0 255.255.255.0 range 192.168.2.167 192.168.2.200 dns-server 192.168.0.1 default-router 192.168.2.3 lease | | | subnet-mask 255.255.255.0 ip dhcp pool NAC-compliant network 192.168.10.0 255.255.255.0 range 192.168.10.167 192.168.3.200 dns-server 192.168.0.1 default-router 192.168.10.3 lease | | | subnet-mask 255.255.255.0 service dhcp-server access-list 3001 permit ip 192.168.10.0/24 any access-list 3002 permit ip 192.168.2.0/24 192.168.0.1/32 access-list 3003 permit ip 192.168.2.0/24 192.168.0.2/32 access-list 3005 permit udp any range 67 68 any range 67 68 access-list 3006 deny ip any any vlan database vlan 2 name noncompliant vlan 10 name compliant interface portI.0.I-I.0.8 switchport switchport mode access interface port1.0.9-1.0.24 switchport switchport mode access ip access-group 3001 ip access-group 3002 ip access-group 3003 ip access-group 3004 ip access-group 3005 ip access-group 3006 dot1x port-control auto dot1x control-direction in auth host-mode single-host auth dynamic-vlan-creation interface vlan l ip address 192.168.0.4/24 interface vlan2 ip address 192.168.2.3/24

> interface vlan3 ip address 192.168.10.3/24

## **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

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

© 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



