

SOPHOS

Sophos NAC for Endpoint Security and Control Installation Guide

Version 3.1.2

Document date: February 2009



Contents

1 About This Document.....	3
2 Installation Checklist.....	4
3 Post-Installation Checklist.....	5
4 System Requirements.....	7
5 Single Server Installation.....	11
6 Multiple Server Installation	12
7 Software Uninstalls.....	15
8 Post-Installation Requirements.....	16
9 Web Agent Installation.....	24
10 Web Agent Uninstall.....	30
11 Agent Deployment.....	31
12 Agent Upgrades.....	33
13 Agent Uninstall.....	34
14 Optional Settings (Multiple Server Installations Only)	35
15 Copyright Statement.....	41

1 About This Document

This document contains information about the following for Sophos NAC:

- Installation and Post-Installation Checklists
- System Requirements
- Software Installation
- Software Uninstalls
- Post-Installation Requirements
- Web Agent System Requirements
- Web Agent Installation
- Web Agent Uninstall
- Agent System Requirements
- Agent Deployment
- Agent Uninstall
- Optional Settings (Multiple Server Installations only)

1.1 Intended Audience

The intended audience for this documentation is an IT generalist for a small business of 100 to 1000 endpoints. The audience may include IT specialists for businesses with more than 1,000 endpoints, not to exceed 25,000 endpoints. If you have more than 1,000 endpoints, Sophos Professional Services are recommended. Professional Services works with your security team to devise and implement a software deployment plan.

1.2 NAC Manager Account Name and Password

To access the NAC Manager, you must use an account name and password.

Use the following account name and password to access the NAC Manager for the first time:

- **Account Name** = admin
- **Password** = a password of your choice

The first time you access the NAC Manager you are required to change the password. Keep a record of this password, because it is the only access to the NAC Manager you have until you create other user accounts. For more information, see [Access the NAC Manager](#) on page 22.

2 Installation Checklist

Important: This version of Sophos NAC requires Sophos Enterprise Console.

Task	Description	Completed
1.	<p>Locate the Windows Server 2003 and/or Windows Server 2000 operating system CDs.</p> <p>Note: The Sophos NAC installation guides you through the installation of the system requirements. The installation may request that the system requirements be installed from an operating system CD.</p>	
2.	<p>Install Sophos NAC.</p> <p>Note: For installations that are 1,000 endpoints or less, Sophos NAC can be installed on the same server as Sophos Enterprise Console. This implementation requires one server running Windows Server 2003. For larger installations, the Sophos NAC application, the Sophos NAC databases, and Sophos Enterprise Console each requires their own server, for a total of three servers. The Sophos NAC application requires Windows Server 2003 and the Sophos NAC database requires Windows Server 2003 or Windows Server 2000 with SP3.</p> <p>Note: If you are using SQL Server 2000 - Desktop Engine Edition (MSDE) for Sophos NAC, Sophos recommends that you install Sophos Enterprise Console prior to installing Sophos NAC. Sophos Enterprise Console installs MSDE.</p>	

3 Post-Installation Checklist

Once the installation completes, you must configure the Sophos Enterprise Console. Sophos NAC DHCP configuration is optional and depends on whether you intend to use DHCP enforcement.

Task	Description	Completed
Sophos NAC Configuration		
1.	<p>Start the SQL Server Agent. (Optional task)</p> <p>For more information see, Start the SQL Server Agent on page 16.</p> <p>Note: This step is not required if you are using SQL Server 2000 MSDE or SQL Server 2005 Express. NAC implementations running on SQL Server 2000 MSDE and 2005 Express do not use the SQL Agent.</p>	
2.	<p>Size the Sophos NAC databases and transaction logs.</p> <p>Note: For installations up to 1500 endpoints, the Sophos NAC installation sizes the NAC databases and transaction logs appropriately. For larger installations, you must increase the sizes of the NAC databases and transaction logs.</p> <p>For more information, see Size the NAC Databases and Transaction Logs on page 16.</p>	
3.	<p>Access the NAC Manager using <code>admin</code> as the account name and a password of your choice.</p> <p>Note: Using the NAC Manager, you can update the pre-configured access templates, profiles, and policies as appropriate.</p> <p>For more information, see NAC Manager on page 22.</p>	
4.	<p>Install the Web Agent on a Web server.</p> <p>Note: This server may be the Sophos NAC server.</p> <p>For more information, see Installation Steps for the Web Agent on a Web Server on page 26.</p>	
Microsoft DHCP Implementation (Optional Task)		
5.	<p>See the Microsoft DHCP Enforcement Guide for a checklist of all DHCP tasks.</p>	

Task	Description	Completed
Sophos Enterprise Console Configuration		
6.	<p>Use the Sophos Enterprise Console to create or import groups.</p> <p>Note: The Sophos Enterprise Console installation attempts to pre-populate the NAC URL with the correct server address. If successful, the NAC Manager opens when you click the NAC toolbar icon in Sophos Enterprise Console. If not successful, you are prompted to type the correct server address when you click the NAC toolbar icon. The Agent uses the NAC URL to communicate with the NAC server. For more information, see the <i>Sophos Endpoint Security and Control network startup guide</i>.</p>	
7.	<p>Use the Sophos Enterprise Console Protect computers wizard to deploy the Sophos NAC Agent to endpoints. For more information, see the <i>Sophos Endpoint Security and Control network startup guide</i>.</p> <p>Note: Install Sophos Anti-Virus and Client Firewall prior to enabling enforcement in Sophos NAC. Sophos NAC defaults to Report Only.</p>	

4 System Requirements

The Sophos NAC installation guides you through the installation of the Sophos NAC system requirements. There are system requirements that must be installed from an operating system CD. You must have the appropriate operating system CD available. Also, a few system requirements are installed automatically by the Sophos NAC installation.

The following system requirements must be installed from the operating system CD if they are not already installed on the server(s):

- Internet Authentication Service (IAS)
- Microsoft Messaging Queue (MSMQ)
- Internet Information Services (IIS) Version 6.0 or higher
- ASP.NET

The following system requirements are installed automatically by the Sophos NAC installation if they are not already installed on the server(s):

- Windows Installer 3.0 or greater
- .NET 2.0
- Microsoft Windows WSE 3.0 for .NET

4.1 Single Server Requirements

NAC Single Server Requirements	
Operating System	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> ■ Windows Server 2003 base and higher (Standard, Enterprise, or Datacenter edition) ■ Windows Server 2003 R2 base and higher (Standard, Enterprise, or Datacenter edition) <p>Note: Sophos NAC does not support 64-bit versions of Windows Server 2003. Also, Sophos NAC installs on foreign operating systems; however, the NAC Manager is in English.</p>
Processors and CPUs	<p>Sophos NAC, Sophos Enterprise Console, and SQL Server on one server for 1000 endpoints:</p> <ul style="list-style-type: none"> ■ 2.0 GHz Pentium or equivalent
Memory	1 GB or more of RAM

NAC Single Server Requirements	
Disk Space	3 GB of free hard disk space on the C drive
SQL Server	<p>The following SQL Server editions are supported:</p> <ul style="list-style-type: none"> ■ SQL Server 2005 - Standard, Workgroup, Enterprise, or Express with SP1 ■ SQL Server 2000 - Standard, Enterprise, Datacenter, or Desktop Engine (MSDE) Edition with SP3a <p>Important: The instance of SQL Server must be running as either Local System or as a valid domain account. Local accounts on the server will not function properly with Sophos NAC.</p>
Protocol	TCP/IP protocol
Internet Access	Internet access is required to download the latest detection information for security applications.
Connectivity	<p>At least one connectivity device must be installed, depending on your connection method:</p> <ul style="list-style-type: none"> ■ Ethernet adapter for a wired broadband connection ■ 802.11 wireless adapter for a wireless broadband connection
Web Certificate (Optional)	Sophos NAC supports HTTPS. For HTTPS, you must install a Web certificate on the NAC server. For more information, see Using HTTPS with Sophos NAC on page 40.

4.2 Multiple Server Requirements

For larger installations, the Sophos NAC application, the Sophos NAC databases, and Sophos Enterprise Console each requires their own server, for a total of three servers. For Sophos Enterprise Console requirements, see the *Sophos Endpoint Security and Control startup guide*.

NAC Multiple Server Requirements	
Domain Controller Requirement	
Sophos NAC Service Account	You must manually create one standard domain account on the domain controller, specify that the password never expires, and specify that the user cannot change the password. To complete this task, you must have a domain administrator account on the domain controller.

NAC Multiple Server Requirements	
	The Sophos NAC installation adds this service account to the local administrators group on the application server so that Sophos NAC can access the NAC databases.
NAC Database Server Requirements	
Operating System	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> ■ Windows Server 2003 base and higher ■ Windows Server 2003 R2 base and higher ■ Windows Server 2000 with SP3 and higher <p>Note: Sophos NAC does not support 64-bit versions of Windows 2003 Server. Also, Sophos NAC installs on foreign operating systems; however, the NAC Manager is in English.</p>
Processors and CPUs	<ul style="list-style-type: none"> ■ 2 GHz or faster Xeons ■ 2 CPUs
Memory	2 GB or more of RAM
Disk Space	3 GB of free hard disk space on the C drive
SQL Server	<p>The following SQL Server editions are supported:</p> <ul style="list-style-type: none"> ■ SQL Server 2005 - Standard, Workgroup, Enterprise, or Express with SP1 ■ SQL Server 2000 - Standard, Enterprise, Datacenter, or Desktop Engine (MSDE) Edition with SP3a <p>Important: The instance of SQL server must be running as either Local System or as a valid domain account. Local accounts on the database server will not function properly with Sophos NAC.</p>
NAC Application Server Requirements	
Operating System	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> ■ Windows Server 2003 base and higher (Standard, Enterprise, or Datacenter edition) ■ Windows Server 2003 R2 base and higher (Standard, Enterprise, or Datacenter edition)

NAC Multiple Server Requirements	
	Note: Sophos NAC does not support 64-bit versions of Windows Server 2003. Also, Sophos NAC installs on foreign operating systems; however, the NAC Manager is in English.
Processors and CPUs	<ul style="list-style-type: none"> ■ 2 GHz or faster Xeons ■ 2 CPUs
Memory	2 GB or more of RAM
Disk Space	<p>80 MB of free hard disk space on the C drive if .NET 2.0 is already installed</p> <p>360 MB of free hard disk space on the C drive if .NET 2.0 must be installed</p>
Protocol	TCP/IP protocol
Internet Access	Internet access is required to download the latest detection information for security applications.
Connectivity	<p>At least one connectivity device must be installed, depending on your intended connection method:</p> <ul style="list-style-type: none"> ■ Ethernet adapter for a wired broadband connection ■ 802.11 wireless adapter for a wireless broadband connection
Web Certificate (Optional)	Sophos NAC supports HTTPS. For HTTPS, you must install a Web certificate on the NAC server. For more information, see Using HTTPS with Sophos NAC on page 40.

5 Single Server Installation

When you install Sophos NAC on a single server, the installation installs the NAC databases first and the NAC application second.

1. Log on as follows:

- If the computer is in a domain, log on as a domain administrator.
- If the computer is in a workgroup, log on as a local administrator.

2. Go to the Sophos website, download the Sophos NAC installer, and run it.

Alternatively, insert the Sophos Install CD. The CD should start automatically.

3. An installation wizard launches. Click **Install**.

4. In the Welcome dialog box, click **Next** to continue.

5. In the Select Features dialog box, click **Next** to continue.

If you are installing the NAC application and NAC databases on separate servers, select the **Advanced** option button and run the NAC installation on each server. For more information, see [Multiple Server Installation](#) on page 12.

6. As appropriate, specify this server's internet proxy settings by selecting an option button. Click **Next**.

If you are using a proxy that is not specified in Sophos Enterprise Console, select the **Use Proxy** option button. If you are using a proxy that is specified in Enterprise Console, select the **Use SEC Proxy Settings** option button. The username, password, and confirm password are required only when the NAC server is using an authenticated proxy.

7. In the Ready to Install dialog box, click **Install**.

Sophos NAC is configured, and the installation progress displays. A portion of the installation takes several minutes, during which time the progress indicator may not move. Do not cancel the installation, and it will progress.

8. Click **Finish**.

Note:

- If installation errors occur, use the Event Log to view additional information. If the NAC database installation fails, you must delete the following databases if they have been created: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreCache, ReportStoreWH, and SecurityStore. Once you have deleted the databases, you can attempt a re-installation.
- Once the installation completes, you must complete the post-installation requirements. For more information, see [Post-Installation Requirements](#) on page 16.

6 Multiple Server Installation

For larger installations, Sophos requires that you install the NAC databases and the NAC application on separate servers. When you install the NAC databases and the NAC application on separate servers, they must be joined to the same domain. Additionally, the NAC databases installation requires that you use a domain account with local administrator privileges. You must install the NAC databases prior to installing the NAC application.

Important: You must manually create one standard domain account on the domain controller, specify that the password never expires, and specify that the user cannot change the password. To complete this task, you must have a domain administrator account on the domain controller. The Sophos NAC installation adds this service account to the local administrators group on the NAC application server so that Sophos NAC has the appropriate rights to perform its required tasks. The service account cannot be a member of the SysAdmin group on the SQL server where you are installing the NAC databases.

6.1 Databases Installation

When you install the NAC databases and the NAC application on separate servers, they must be joined to the same domain. Additionally, the NAC databases installation requires that you use a domain account with local administrator privileges.

1. On the domain controller, manually create one standard domain account, specify that the password never expires, and specify that the user cannot change the password.

The NAC installation adds this service account to the local administrators group on the NAC application server so that the NAC Manager can access the NAC databases.

2. Go to the Sophos website, download the Sophos NAC installer, and run it.
Alternatively, insert the Sophos Install CD. The CD should start automatically.
3. An installation wizard launches. Click **Install**.
4. In the Welcome dialog box, click **Next**.
5. In the Select Features dialog box, select the **Advanced** option button.
6. Select the **Sophos NAC Databases** check box. Clear all other check boxes. Click **Next**.
If you want to change the directory where the scripts that create the NAC databases are installed, click **Browse**. If you want to change the SQL server instance that NAC will use, click **Select**. The Select button only appears when the NAC installer detects more than one SQL server instance.
7. Type the Service Account Information in the appropriate fields. Click **Next** to continue.
This is the standard domain account required by the SQL server and the NAC application. This service account was created in step 1.

8. On the Ready to Install dialog box, click **Install** to begin the installation.

The NAC databases are configured, and the installation progress displays. A portion of the installation takes several minutes, during which time the progress indicator may not move. Do not cancel the installation, and it will progress.

9. Click **Finish**.

Important: If installation errors occur, use the Event Log to view additional information. If the NAC database installation fails, you must delete the following databases if they have been created: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreCache, ReportStoreWH, and SecurityStore. Once you have deleted the NAC databases, you can attempt a re-installation.

6.2 Application Installation

When you install the NAC databases and the NAC application on separate servers, they must be joined to the same domain. Additionally, the application installation requires that you use a domain account with local administrator privileges.

1. Go to the Sophos website, download the Sophos NAC installer, and run it.
Alternatively, insert the Sophos Install CD. The CD should start automatically.
2. An installation wizard launches. Click **Install**.
3. In the Welcome dialog box, click **Next**.
4. Do one of the following:
 - If a message indicates that the NAC Application Server is the only NAC server that can be installed, click **OK**. In the **Select Features** dialog box, click **Next**.
 - If the **Select Features** dialog box displays, select the **Advanced** option button. Clear all check boxes, and then select the **Sophos NAC Application Server** check box. Click **Next**.

If you want to change the directory where the NAC Application Server files are installed, click **Browse**.

5. Type the Service Account Information in the appropriate fields. Click **Next** to continue.

Note: This service account information must match the service account information you entered when you installed the Sophos NAC databases.

6. Type the Sophos NAC database server name. Click **Next** to continue.

This is the standard domain account required by the SQL server and the NAC Manager. This service account information must match the service account information you entered when you installed the NAC databases.

7. As appropriate, specify this server's internet proxy settings by selecting an option button. Click **Next**.

If you are using a proxy that is not specified in Sophos Enterprise Console, select the **Use Proxy** option button. If you are using a proxy that is specified in Enterprise Console, select the **Use SEC Proxy Settings** option button. The username, password, and confirm password are required only when the NAC server is using an authenticated proxy.

8. Click **Install** to begin the installation.

The NAC application is configured, and the installation progress displays. A portion of the installation takes several minutes, during which time the progress indicator may not move. Do not cancel the installation, and it will progress.

9. Click **Finish**.

- If installation errors occur, use the Event Log to view additional information.
- Once the installation completes, you must complete the post-installation requirements. For more information, see [Post-Installation Requirements](#) on page 16.

6.3 Software Upgrades

For information on upgrading Sophos NAC for Endpoint Security and Control, see the *Sophos NAC for Endpoint Security and Control Upgrade Guide*. Sophos NAC for Endpoint Security and Control does **not** support upgrades to Sophos NAC Advanced. You must first uninstall Sophos NAC for Endpoint Security and Control. This uninstall includes all Sophos NAC Agents. Then you can install Sophos NAC Advanced.

7 Software Uninstalls

When you uninstall Sophos NAC, you must uninstall the NAC application first and the NAC databases second; otherwise, the NAC application will produce errors because the NAC databases have been uninstalled.

7.1 NAC Application Uninstall

Uninstalling the NAC application does not delete any items you have created in the NAC Manager. All items, such as policies and user account information, are stored in the NAC databases.

1. From the Start menu, click **Control Panel > Add or Remove Programs** .
2. Select **Sophos NAC Application Server** and click **Remove**.
3. Click **Yes** to confirm the removal of the application. The application is removed.

7.2 NAC Database Uninstall

Uninstalling the NAC databases removes only the files that were used to create the databases and not the actual databases themselves.

1. From the Start menu, click **Control Panel > Add or Remove Programs** .
2. Select **Sophos NAC Databases** and click **Remove**.
3. Click **Yes** to confirm the removal of the server files that were used to create the NAC databases. The server files are removed, and the NAC databases remain intact.

8 Post-Installation Requirements

The post-installation requirements are additional configuration processes that are required for Sophos NAC to work properly.

8.1 Start the SQL Server Agent

The NAC Manager Reports area enables you to generate reports that help identify security compliance risks of endpoints. These reports generate common reporting searches that can assist in troubleshooting. For report generation to succeed, you must verify that the SQL Server Agent is started.

Note: These instructions apply to all supported databases except SQL Server 2000 MSDE and 2005 Express. NAC implementations running on SQL Server 2000 MSDE and 2005 Express do not use the SQL Agent.

1. From the Start menu on the SQL server, do one of the following:
 - If you are using SQL Server 2000, click **Microsoft SQL Server > Enterprise Manager** . SQL Enterprise Manager opens.
 - If you are using SQL Server 2005, click **Microsoft SQL Server 2005 > SQL Server Management Studio** . SQL Server Management Studio opens.
2. To start the SQL Server Agent, do one of the following:
 - If you are using SQL Server 2000, under the Management folder, locate **SQL Server Agent**, right-click it and select **Start**.
 - If you are using SQL Server 2005, locate **SQL Server Agent**, right-click it and select **Start**.

Important: To ensure that the SQL Server Agent starts automatically when the SQL server restarts, you must access the Windows Services Control Manager and change the Startup Type of the SQLSERVERAGENT service (SQL Server 2000) or the SQL Server Agent (SQL Server 2005) service to automatic.

3. Exit SQL Enterprise Manager or SQL Server Management Studio.

8.2 Size the NAC Databases and Transaction Logs

The installation creates the NAC databases to permit auto grow, prevent auto shrink, and automatically update statistics. Sophos recommends that you do not change these default NAC database properties.

For the best NAC database performance, Sophos recommends that you:

- Size the NAC databases and the appropriate transaction logs large enough so that they do not expand frequently.

Note: For installations up to 1500 endpoints, the Sophos NAC installation sizes the NAC databases and transaction logs appropriately. For larger installations, you must increase the sizes of the NAC databases and transaction logs.

Note: Installations up to 1500 endpoints typically use SQL Server MSDE or SQL Server 2005 Express for the NAC Databases. If you have over 1500 users, Sophos recommends using SQL Server 2000 or 2005 for the NAC Databases. SQL Server MSDE databases are limited to 2 GB and 2005 Express databases are limited to 4 GB.

8.2.1 Database Sizing Guidelines

Use this table to determine how to specify the size of the ReportStore database.

Number of Endpoints	ReportStore Database Size Guidelines
1,500	300 MB
5,000	485 MB
7,500	616 MB
10,000	748 MB
15,000	1011 MB
20,000	1274 MB
25,000	1536 MB

8.2.2 Transaction Log Sizing Guidelines

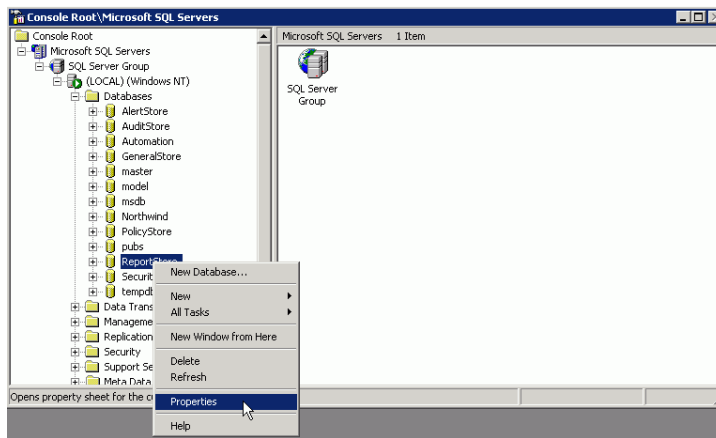
Use this table to determine how to specify the size of the ReportStore transaction log.

Number of Endpoints	ReportStore Log Size Guidelines
1,500	150 MB
5,000	281 MB
7,500	374 MB
10,000	467 MB
15,000	653 MB
20,000	839 MB
25,000	1024 MB

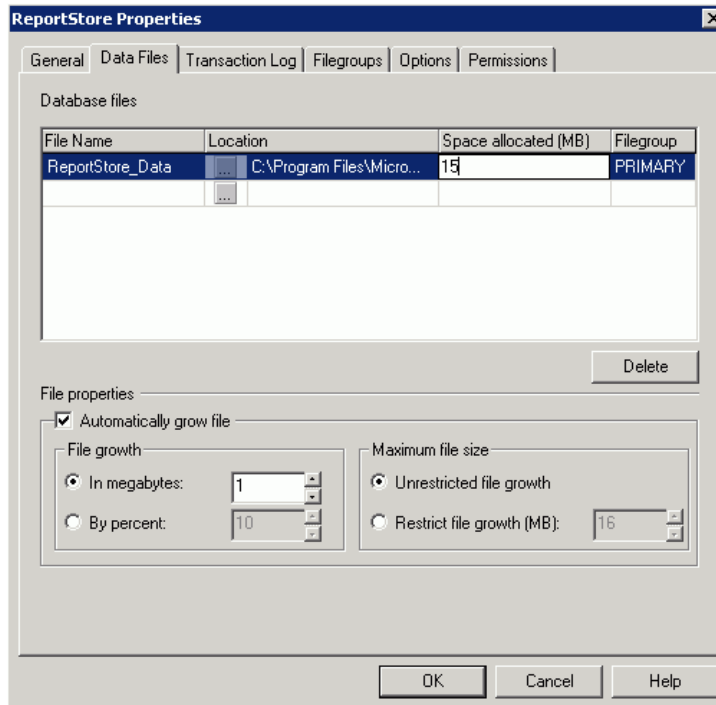
8.2.3 Changing the NAC Database and Transaction Log Sizes (SQL Server 2000)

To determine the NAC database and transaction log sizes, see [Database Sizing Guidelines](#) on page 17 and [Transaction Log Sizing Guidelines](#) on page 17. The following instructions apply to SQL Server 2000.

1. From the SQL Server Start menu, click **Microsoft SQL Server > Enterprise Manager** .
SQL Enterprise Manager opens.
2. To size the ReportStore, under the Databases folder, locate **ReportStore**, right-click and select **Properties**.

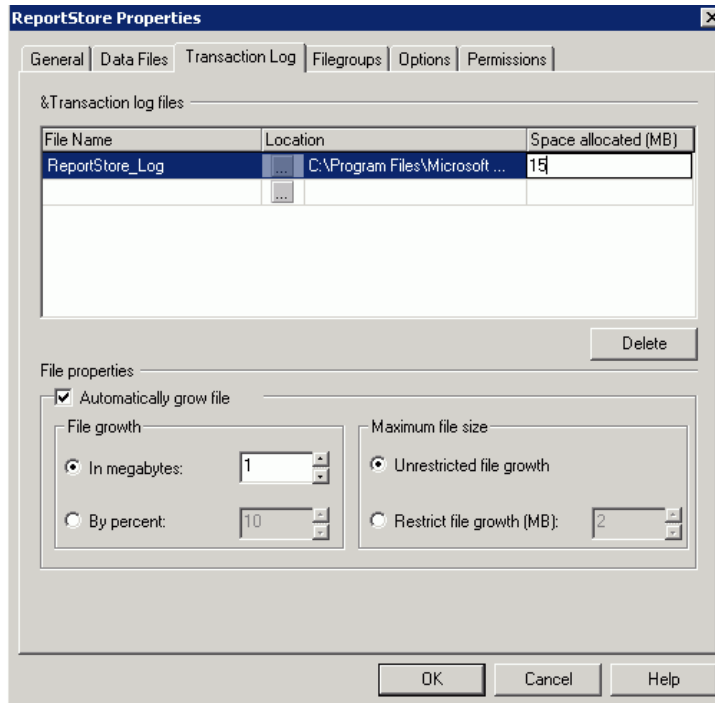


3. Click the **Data Files** tab.



4. Select the **Space allocated (MB)** field, and type an appropriate size for the ReportStore.
5. Select the **In megabytes** option button, and then type an appropriate size for the ReportStore file growth.

6. Click the **Transaction Log** tab.

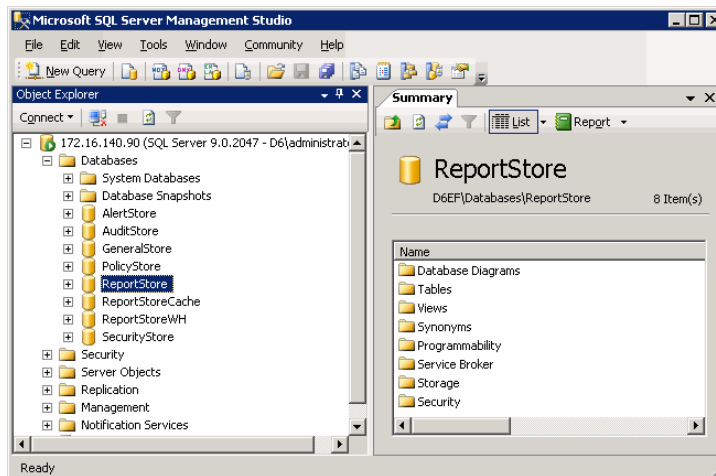


7. Select the **Space allocated (MB)** field, and then type an appropriate size for the ReportStore transaction log.
8. Select the **In megabytes** option button, and then type an appropriate size for the ReportStore transaction log file growth.
9. Click **OK**.
10. Exit SQL Enterprise Manager.

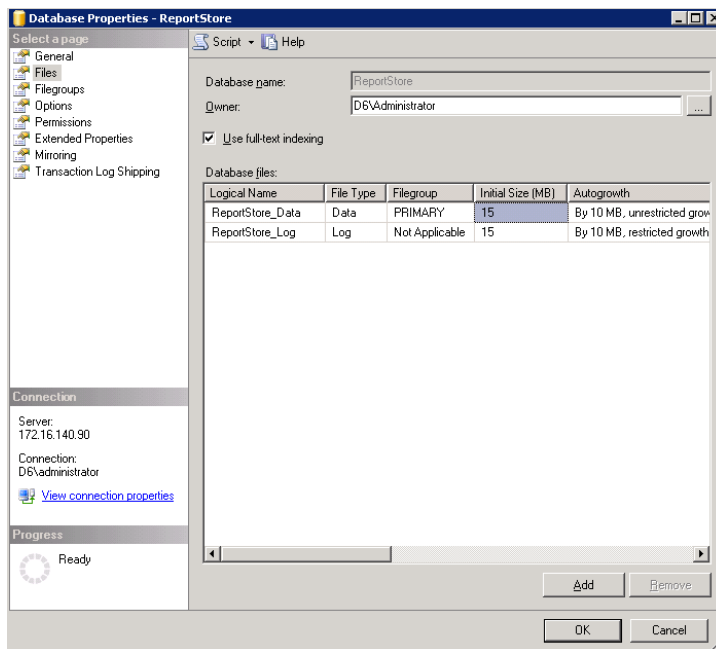
8.2.4 Changing the NAC Database and Transaction Log Sizes (SQL Server 2005)

To determine the NAC database and transaction log sizes, see [Database Sizing Guidelines](#) on page 17 and [Transaction Log Sizing Guidelines](#) on page 17. The following instructions apply to SQL Server 2005.

1. From the SQL Server Start menu, click **Microsoft SQL Server 2005 > SQL Server Management Studio** .



2. From the SQL Server Management Studio dialog box, locate the **ReportStore** database in the Databases folder, right-click and select **Properties**.



3. From the Properties dialog box, select **Files**.

4. Locate the **ReportStore_Data** file, select the **Initial Size (MB)** field, and type an appropriate size for the database.
5. Locate the **ReportStore_Log** file, select the **Initial Size (MB)** field, and type an appropriate size for the log file.
6. Click **OK**.
7. Exit SQL Server Management Studio.

8.3 Access the NAC Manager

The NAC Manager provides a centralized location for policy definition and endpoint compliance reporting. The NAC Manager installs as a Default Web Site in following location:

<LocalDrive>\Inetpub\wwwroot\SophosNAC, unless you changed the location during installation.

Important: For the NAC Manager to display and save information and to display graphics appropriately, you must:

- Add the NAC Manager as a trusted Web site in Internet Explorer 6.x. This setting is not needed for Internet Explorer 7.x.
- Turn off pop-up blocking when you access the NAC Manager.

Note: Since you have installed Sophos NAC as part of Sophos Endpoint Security and Control, you can access the NAC Manager from Sophos Enterprise Console. For more information, see the *Sophos Endpoint Security and Control network startup guide*.

1. Open Internet Explorer.
2. Type the following address: `http(s)://<ip address/DNS of the Sophos NAC server>/SophosNAC`. The NAC Manager Logon page appears.
3. Type Admin in the **Account Name** field and a password of your choice in the **Password** field.

4. Click **OK**.

Note:

- The first time you access the NAC Manager you are required to change the password. Keep a record of this password, because it is the only access to the NAC Manager you have until you create other user accounts.
- Using the NAC Manager, you can update the pre-defined access templates, profiles, and policies as appropriate.
- Once you have installed Sophos Enterprise Console, you must use Sophos Enterprise Console to create or import groups. For more information, see the *Sophos NAC Manager Guide* or the *Sophos Endpoint Security and Control network startup guide*.
- The Sophos Enterprise Console installation attempts to pre-populate the NAC URL with the correct server address. If successful, the NAC Manager opens when you click the NAC toolbar icon in Sophos Enterprise Console. If not successful, you are prompted to type the correct server address when you click the NAC toolbar icon. The Agent uses the NAC URL to communicate with the NAC server. For more information, see the *Sophos Endpoint Security and Control network startup guide*.

9 Web Agent Installation

The Web Agent installs from a separate Web Agent msi file. Install the Web Agent on a Web server that is accessible to endpoints that must use the Web Agent. The Web Agent may be installed on the same server as Sophos NAC.

9.1 Web Agent Web Server System Requirements

Web Server Hosting Web Agent Requirements

The following must be installed and running on the server prior to installing the Web Agent:

- Internet Information Services (IIS).
- 10 MB of free hard disk space.

Web Agent Components Installed on Web Server

- Web Agent CAB files that control the Agent's functionality.
- Web Agent host page that controls the front-end of the Web Agent interface.
- Web Agent branding file (webagent.css) that controls style and format.
- Web Agent graphic files that display on the Web Agent interface.

9.2 Web Agent Endpoint System Requirements

Endpoint System Requirements

The following are the system requirements that are necessary to use the Web Agent:

- Microsoft Windows operating system
 - Windows 2000 SP3 and higher
 - Windows XP SP1 and higher
 - Windows Vista Enterprise and Business base and higher

Note: The Web Agent does not support installations on server operating systems.

- Microsoft Windows supported platforms (English, French, Spanish, German, Italian, Japanese, Simplified Chinese, and Traditional Chinese).
- Microsoft Internet Explorer 5.0 or greater.

Internet Explorer Security Settings Requirements for Endpoints

The following are the required Internet Explorer 5.0 or greater security settings that must be specified for the correct Web content zone. The correct Web content zone depends on where you install Web Agent.

- Run components signed with Authenticode must be enabled.

- Automatic prompting for ActiveX controls must be enabled.
- Download signed ActiveX controls must be enabled.
- Run ActiveX controls and plug-ins must be enabled.
- Script ActiveX controls marked safe for scripting must be enabled.
- On endpoints running Internet Explorer 7.x, the server where the Web Agent is installed must be specified as a trusted site. Additionally, Protected Mode must be disabled on Vista.

Important: For all operating systems, administrative rights are required on the endpoint to download the Web Agent. As implemented by Microsoft, the restricted user mode cannot download ActiveX controls.

Additional Internet Explorer Security Setting Requirements for Endpoints Running Vista

- User Account Control (UAC) must be turned on.
- ActiveX Installer Service must be installed and set to run automatically.

Note: You can install the ActiveX Installer Service from **Control Panel > Programs and Features > Turn Windows features on and off**. Under services, the ActiveX Installer Service is named AxInstSV. You must restart the endpoint after you install and set the service to run automatically.

- Group policy setting for ActiveX controls must be enabled (located at **Computer Configuration > Administrative Templates > Windows Components > ActiveX Installer Service > Approved Installation Sites for ActiveX Controls**), the URL for the Web Agent must be added, and a value of 2,1,0,0 must be added.

Note: Type the URL into the **Enter the name of the item to be added** field and type the value **2,1,0,0** into the **Enter the value of the item to be added** field.

Note: The value 2,1,0,0 is derived from the following information. The first three digits indicate how the ActiveX control should be installed based on the signature. The first digit is for trusted controls, the second digit is for signed controls, and the third digit is for unsigned controls. The possible values are: 0 = do not install, 1 = prompt user to install, and 2 = silent install. The silent install is not permitted for unsigned controls. The last digit is a bitmask flag indicating whether or not to ignore HTTP certificate errors. The possible values are: 0 = no certificate errors (default), 256 = ignore unknown CA, 4096 = ignore unknown CN, 8192 = ignore invalid certificate date, and 512 = ignore wrong certificate usage.

Endpoint Downloaded Components

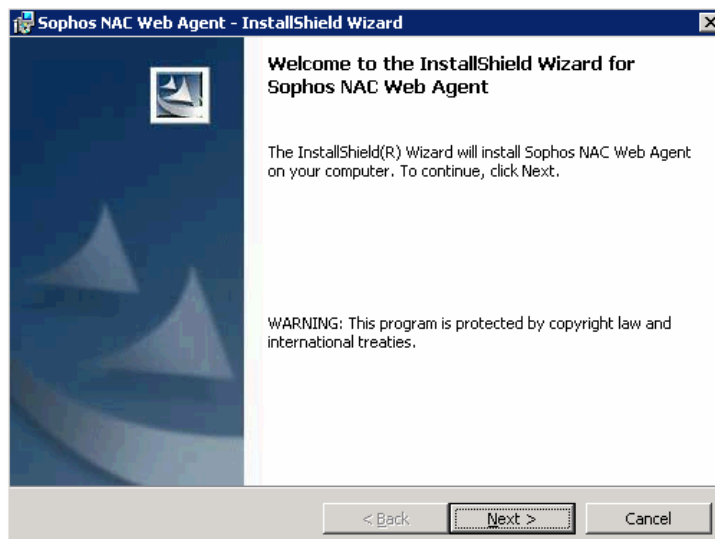
- **%tmp%\Sophos\NAC Directory:** The Sophos NAC subdirectory is beneath a temporary directory that is configured for the user. By default, the temporary directory is unique for each user. Use the following methods to locate the temporary directory: the path specified by the TEMP environment variable, the path specified by the USERPROFILE environment variable, or the Windows directory.
 - Data Files

- Logs
- **c:\Windows\Download Program Files:** The directory where the Web Agent ActiveX controls are downloaded and installed on an endpoint.
 - AgentObj Class
 - CredListObj Class
- **Microsoft Visual C++ Redistributable Package:** The package provides libraries required to run the Web Agent on the supported operating systems.

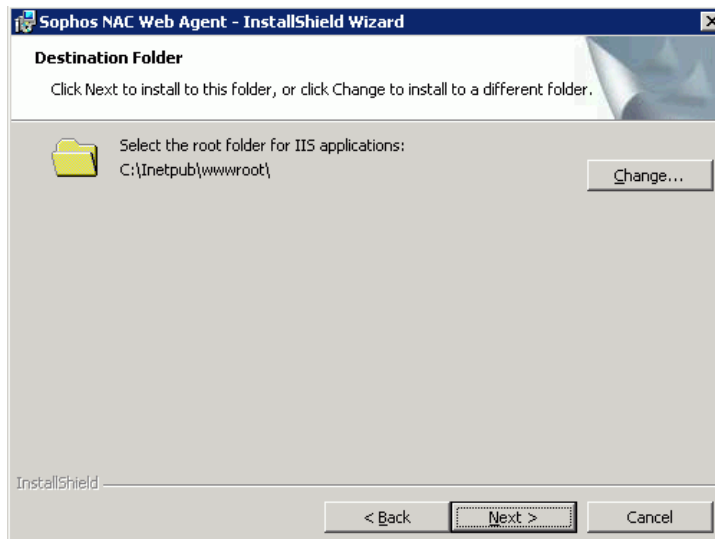
9.3 Installation Steps for the Web Agent on a Web Server

Install the Web Agent after you complete the *Post-installation Requirements* section of this document. The Web Agent may be installed on the server where you installed Sophos NAC or another Web server.

1. Do one of the following:
 - Locate the Sophos NAC WebAgent.msi on the Sophos Endpoint Security and Control CD.
 - Download Sophos NAC WebAgent.msi from the Sophos website.
2. Double-click the **Sophos NAC Web Agent.msi** file to run the Web Agent installation.
3. Click **Next** to continue.

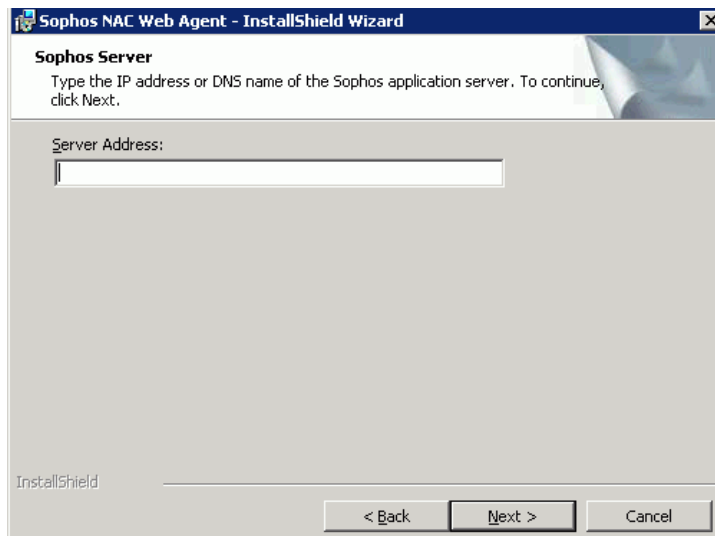


4. Click **Change** to select the appropriate installation directory, or keep the default c:\inetpub\wwwroot directory. Click **Next** to continue.



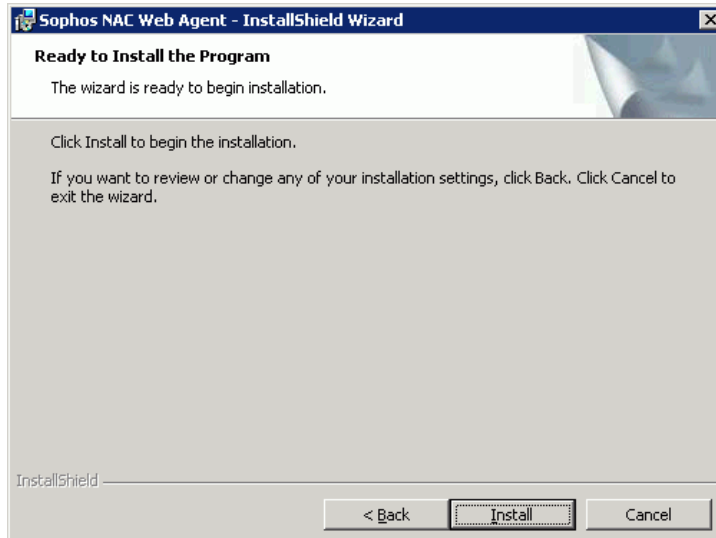
5. Type the Sophos NAC server IP address or DNS name.

Note: If Sophos NAC was installed on more than one server, the server address is the IP address or DNS name of the NAC application server and not the NAC database server.

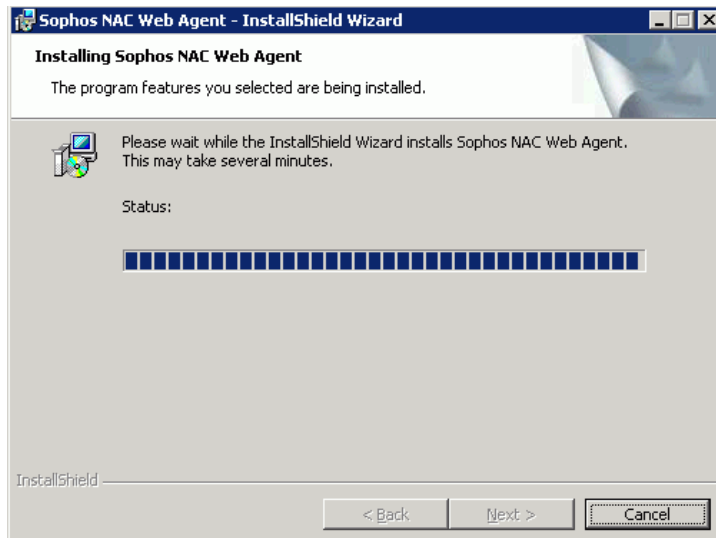


6. If you are using HTTPS, select the **Secure Sophos Server (use HTTPS)** check box. Click **Next** to continue.

7. Click Install to begin the installation.



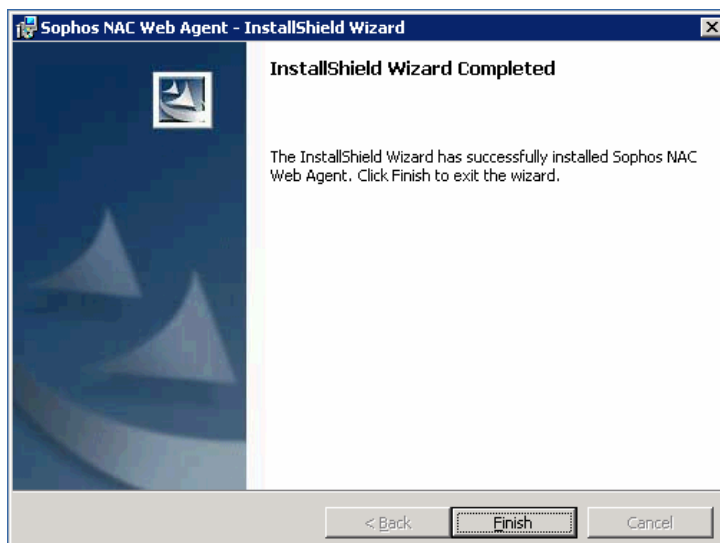
The Web Agent is installed, and the installation progress displays.



8. Click **Finish** to complete the installation.

Note: When installation errors occur, use the Event Log on the Web server to view additional information.

Note: Endpoints can access the Web Agent using the following URL: `http(s)://<ip address/DNS name>/webagent` if you installed the Web Agent to the default directory. The IP address or DNS name is the Web server where you installed the Web Agent.



10 Web Agent Uninstall

Use these steps to uninstall the Web Agent from a Web server.

1. From the Start menu, select **Control Panel > Add or Remove Programs** .
2. Select **Sophos NAC Web Agent**, and then click **Remove**.
3. Click **Yes** to confirm the removal of the Web Agent.

11 Agent Deployment

Once you have completed the *Post-installation Requirements* section of this document and have used Sophos Enterprise Console to create or import groups, you can deploy Agents to endpoints using the Protect computers wizard. For more information, see the *Sophos Endpoint Security and Control network startup guide*.

Note: The Sophos Enterprise Console installation attempts to pre-populate the NAC URL with the correct server address. If successful, the NAC Manager opens when you click the NAC toolbar icon in Sophos Enterprise Console. If not successful, you are prompted to type the correct server address when you click the NAC toolbar icon. The Agent uses the NAC URL to communicate with the NAC server.

- **NAC URL:** This URL is the IP address or DNS name of the Sophos NAC server. If Sophos NAC was installed on more than one server, this URL is the IP address or DNS name of the NAC application server and not the NAC database server.

11.1 System Requirements

The following are the system requirements for the Agent:

Endpoint Requirements	
Supported Operating Systems	Microsoft Windows operating systems: <ul style="list-style-type: none"> ■ Windows 2000 SP3 and higher ■ Windows XP SP1 and higher ■ Windows Vista Enterprise and Business base and higher <p>Note: The Agent does not support installations on server operating systems or 64-bit operating systems.</p>
Supported Platforms	Microsoft Windows supported platforms (English, French, Spanish, German, Italian, Japanese, Simplified Chinese, and Traditional Chinese)
Processor	700 Mhz or faster Pentium processor
Memory	512 MB or more of RAM
Disk Space	20 MB of free hard disk space
Browser	Microsoft Internet Explorer 5.0 or greater
Installed Microsoft Windows Components	Microsoft Windows Installer 2.0 or greater Microsoft XMLDOM 3,4 or 6

11.2 Installed Components

The following components are installed on the endpoint:

- Agent API, as a service.
- Agent Quarantine Manager, as a device driver.
- Agent Application Quarantine Manager, as a device driver.
- Agent graphical user interface, as an executable.
- Microsoft C++ Runtime Library 8.0.
- Assessment DLLs.
- Default.skn file.

11.3 Installation Logging

Agent installation provides logging automatically. If the Agent encounters an error during installation or the installation fails, the log provides troubleshooting information.

The Agent installation log is located in the %tmp% directory. Unless you have altered the location of the temp directory, you can access the directory by opening Windows Explorer, typing %tmp% in the address field, and pressing **Enter**.

12 Agent Upgrades

If you are subscribed to the Sophos Endpoint Security and Control package and you have previously installed Sophos NAC, all endpoints will receive the NAC Agent upgrade automatically. No additional tasks are required. If you have Sophos Endpoint Security and Control already installed, but you are installing Sophos NAC for the first time, see the *Sophos Endpoint Security and Control network upgrade guide*.

13 Agent Uninstall

Important: During an Agent uninstall, a Windows Explorer dialog box may display and require you to close certain applications, such as Microsoft Outlook, prior to uninstalling the Agent. Sophos recommends that you close the applications for a successful uninstall. Also, the Agent uninstall requires the endpoint to restart.

1. From the Start menu, select **Control Panel > Add or Remove Programs** .
2. Select **Sophos NAC**, and then click **Remove**.
3. Click **Yes** to confirm the removal of the Agent.

14 Optional Settings (Multiple Server Installations Only)

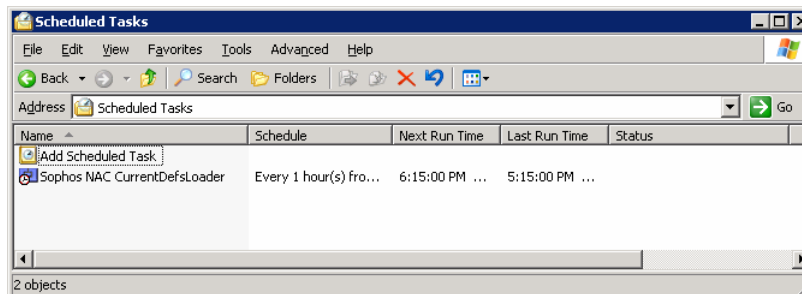
This section contains optional settings for Sophos NAC. This section is intended for multiple server installations.

14.1 Verify/Change the CurrentDefsLoader Task

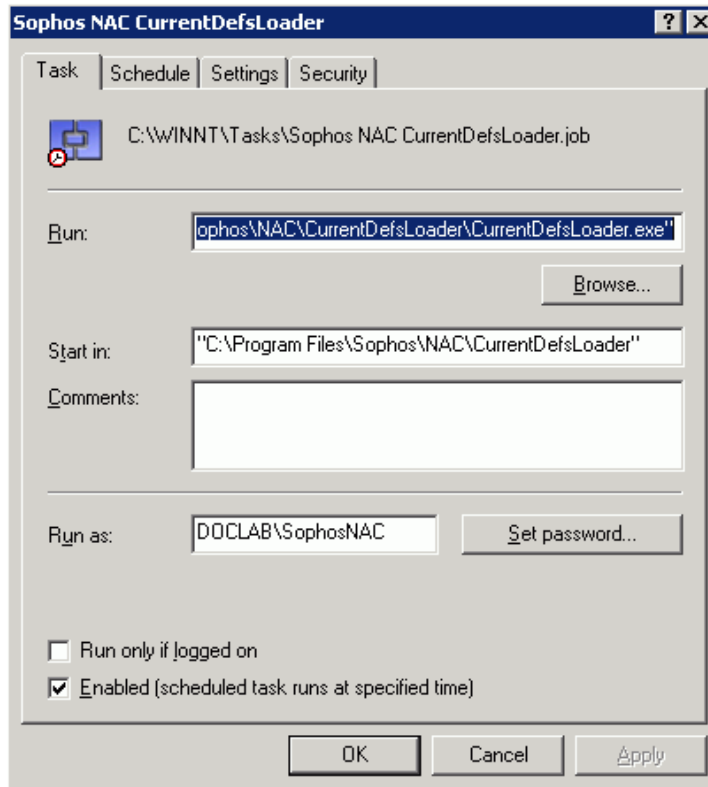
The CurrentDefsLoader task is scheduled to run hourly. The installation schedules this task to run randomly, it takes a few minutes to complete, and it requires Internet access. This task retrieves the latest dates for the current signature for every anti-virus and anti-spyware application.

1. From the application server Start menu, click **Control Panel > Scheduled Tasks** .

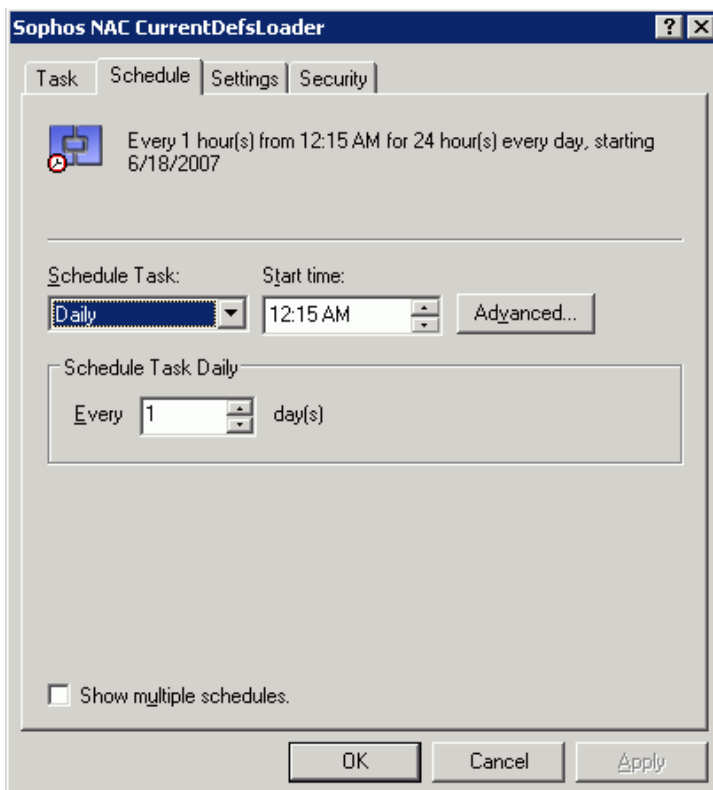
Scheduled Tasks opens.



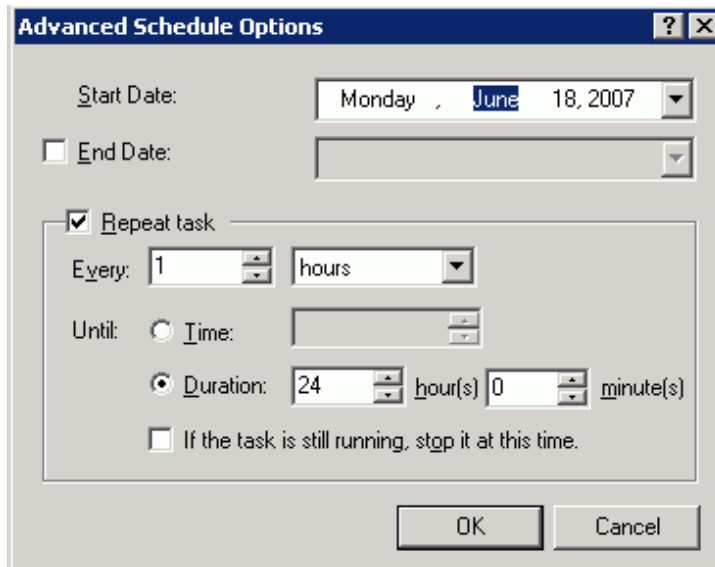
2. Double-click **Sophos NAC CurrentDefsLoader**. The Properties window displays.



3. Click the **Schedule** tab.



4. Click **Advanced**.



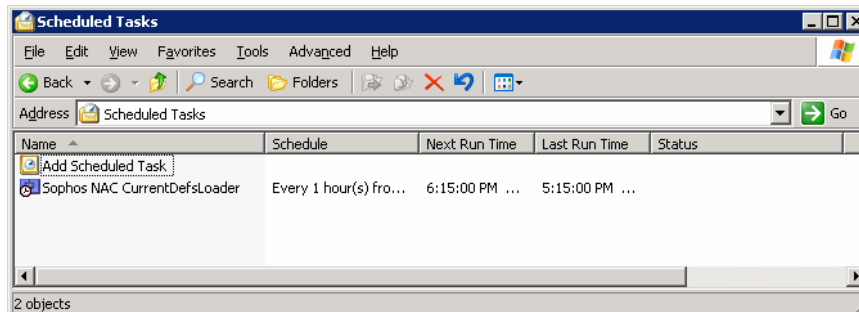
5. As needed, change the time of the scheduled task, and then click **OK**.
6. Click **OK** to save the changes.
7. Exit Scheduled Tasks.

14.2 Run the CurrentDefsLoader Task Manually

The CurrentDefsLoader task is scheduled hourly; however, you can manually run the CurrentDefsLoader task. The installation schedules this task to run randomly, it takes a few minutes to complete, and it requires Internet access. This task retrieves the latest dates for the current signature for every anti-virus and anti-spyware application.

1. From the application server Start menu, click **Control Panel > Scheduled Tasks**.

The Scheduled Tasks opens.



2. Right-click **Sophos NAC CurrentDefsLoader**, and then select **Run**.

Note: Verify that the task ran without error by accessing the Event Log on the NAC server.

3. Exit Scheduled Tasks.

14.3 Verify/Change the Sophos NAC - LoadWH Task

The Sophos NAC - LoadWH is scheduled to run at 2:30 AM each day by default; however, you can manually run the Sophos NAC- LoadWH task. This task controls when the report data is purged.

These instructions apply to all supported databases except SQL Server 2000 MSDE and SQL Server 2005 Express. To change the Sophos NAC - LoadWH task for SQL Server 2000 MSDE and SQL Server 2005 Express, you need to change the Sophos NAC - LoadWH task within the Windows Task Scheduler.

1. From the SQL Server Start menu, do one of the following:
 - If you are using SQL Server 2000, click **Microsoft SQL Server > Enterprise Manager** . SQL Enterprise Manager opens.
 - If you are using SQL Server 2005, click **Microsoft SQL Server 2005 > SQL Server Management Studio** . SQL Server Management Studio opens.
2. Locate the **SQL Server Agent**.
- Note:** If you are using SQL Server 2000, the SQL Server Agent is under the Management folder.
3. Under SQL Server Agent, select **Jobs**.
4. Double-click the **Sophos NAC - LoadWH** task. The Properties window displays.
5. Do one of the following:
 - If you are using SQL Server 2000, click the **Schedules** tab.
 - If you are using SQL Server 2005, click **Schedules**.
6. Do one of the following:
 - Click **New Schedule** (SQL Server 2000) or **New** (SQL Server 2005) to add an additional schedule, add the additional schedule, and then click **OK**.
 - Click **Edit** to edit the existing schedule, edit the existing schedule, and then click **OK**.
7. Click **OK** to save the changes.
8. Exit SQL Enterprise Manager or SQL Server Management Studio.

14.4 Run the Sophos NAC - LoadWH Task Manually

The Sophos NAC - LoadWH task controls when the report data is purged. The default setting runs once a day at 2:30 A.M.; however, you can manually run the Sophos NAC - LoadWH task.

These instructions apply to all supported databases except SQL Server 2000 MSDE and SQL Server 2005 Express. To run the Sophos NAC - LoadWH task manually for SQL Server 2000 MSDE and SQL Server 2005 Express, you need to start the Sophos NAC - LoadWH task within the Windows Task Scheduler.

1. From the SQL Server Start menu, do one of the following:
 - If you are using SQL Server 2000, click **Microsoft SQL Server > Enterprise Manager** . SQL Enterprise Manager opens.
 - If you are using SQL Server 2005, click **Microsoft SQL Server 2005 > SQL Server Management Studio** . SQL Server Management Studio opens.
2. Locate the **SQL Server Agent**.

Note: If you are using SQL Server 2000, the SQL Server Agent is under the Management folder.
3. Under SQL Server Agent, select **Jobs**.
4. Right-click **Sophos NAC - LoadWH**, and then select **Start Job**.

Note: The Sophos NAC - LoadWH task takes approximately the same amount of time to run manually as it takes to run automatically each night.
5. Exit SQL Enterprise Manager or SQL Server Management Studio.

14.5 Using HTTPS with Sophos NAC

Sophos NAC supports HTTPS communication between the NAC server and the NAC Agent.

To use HTTPS, you must do the following:

- Install a Web certificate on the Sophos NAC server prior to installing Sophos Enterprise Console.
- If using the Web Agent, select the Secure Sophos Server (use HTTPS) check box during the Web Agent installation.

Sophos Enterprise Console automatically configures the NAC Agent with the NAC server URL when you use the Protect computers wizard.

15 Copyright Statement

Copyright © 2009 Sophos Group. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

All other product and company names are trademarks or registered trademarks of their respective owners.