

SOPHOS

Sophos NAC for Endpoint Security and Control Tools Guide

Version 3.1.2

Document date: February 2009



Contents

1 About This Document.....	3
2 Loader Tool.....	4
3 Logging Tool.....	7
4 Maintenance Mode Tool.....	12
5 Copyright Statement.....	14

1 About This Document

This document contains information about the following for Sophos NAC:

- Loader Tool
- Logging Tool
- Maintenance Mode Tool

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.

2 Loader Tool

The Loader tool, which is installed as part of Sophos NAC, enables administrators to import new and updated applications and application types to their Sophos NAC databases.

2.1 Importing Applications

There are two ways to import applications using the Loader tool. Administrators can use the application definitions EXE file that calls the Loader tool and automatically imports the applications, or administrators can use a command line to import applications using an import.xml file. Sophos recommends using the application definitions EXE file because it automatically calls the Loader and makes importing applications and application types easier than using a command line. Sophos makes the application definitions EXE file available to all enterprises.

2.1.1 Importing Applications Using the Application Definitions EXE File

1. Download the application definitions EXE file from Sophos.
2. Copy the downloaded application definitions EXE file to the Sophos NAC server.
3. Double-click the application definitions file to import the updated applications and application types.

Note: The application definitions file calls the Loader tool and automatically installs the updated applications and application types.

2.1.2 Manually Importing Applications Using an import.xml File

1. Receive an updated import.xml file from a Sophos representative.
2. Copy the import.xml file to the Sophos NAC server.

3. From a command prompt, run the Loader tool to import the new definitions by typing:
`c:\Program Files\Sophos\NAC\Loader\Loader.exe C:\import.xml.`

Note:

- Commands are not case-sensitive. Command parameters use forward slashes /, and then the parameter name, optionally followed by a colon and parameter value. For example, /ID:id. Parameter values can contain backward slashes \ and spaces; however, any DOS parameter value that contains a space requires quotes, for example: "c:\temp\my key.xml".
- The Loader tool assumes that you are logged on to Windows using a Windows account that has SQL access privileges. If you are not logged on to Windows using an account that has SQL access privileges, you can run the Loader tool using the following for a SQL account: `Loader /L:SQL /ID:ID /PW:PW /F:import.xml` (where ID and PW are the ID and password of a valid SQL account).
- In addition to the DOS commands outlined in the following section, you can view additional options in the Loader tool by typing: `loader /?`.
- By default, any errors that are displayed are also written to the Event Log.

2.2 Exporting Applications

If Sophos needs to see custom application definitions, you must run the Loader tool from a command prompt to export the data to send to Sophos. Use the following examples to export custom applications.

Commands	Descriptions
<code>Loader /A:export /B:application /I:id /F:export.xml</code>	Exports an application by unique ID. The application definition is saved in the XML file specified.
<code>Loader /A:export /B:application /N:"name" /F:export.xml</code>	Exports an application by name. The application definition is saved in the XML file specified.
<code>Loader /A:export /B:application /n:* /F:export.xml</code>	Exports all applications to the XML file specified.

2.3 Loader DOS Commands

The following table lists the DOS commands that can be used with the Loader tool. These commands can be used to load applications into the databases, export applications from the databases, or validate an import.xml file before importing. To use these commands, pass them to the Loader tool as command line parameters. For example, the first command in the table is executed by typing the following in the command line: `Loader /F:import.xml`.

Commands	Descriptions
/F:import.xml	Loads any application or application type from the XML file specified.
/F:imp* .xml	Loads applications or application types from multiple files.
/B:application /N:"name" /F:export.xml	Exports an application by name. The application definition is stored in the XML file specified.

3 Logging Tool

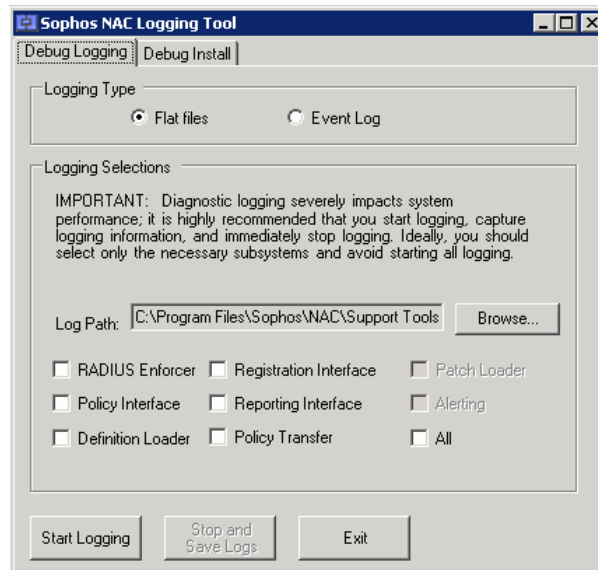
The Logging Tool enables you to turn on installation and subsystem logging in order to perform assisted troubleshooting. The Debug Logging tab enables you to identify the logging method and file location and to manually start and stop logging for selected subsystems. The Debug Install tab enables you to identify the installation file to diagnose and the logging file location. Logging is set at a maximum level; the information logged is dependent on the type of logging performed.

Important: Sophos recommends that you use this tool for troubleshooting purposes only, preferably when guided by a Sophos representative, and that you do not leave logging enabled since it can severely impact system performance.

3.1 Sophos NAC Server Subsystem Logging

1. Locate the Logging Tool on the Sophos NAC server. The default location of this tool is `c:\Program Files\Sophos\NAC\Support Tools`.
2. Double-click **LoggingUtil.exe**.

The Logging Tool, Debug Logging tab displays:



3. Select the appropriate logging type and logging selections, and then click **Start Logging**.

For information about each field, see [Debug Logging Tab Fields and Descriptions](#) on page 8.

Note: Once you click the Start Logging button, you cannot select or de-select additional subsystems. You must stop logging, change your logging selections, and start logging again.

4. Perform appropriate tasks on the server for which you want to capture logging information.

- Once you have performed the appropriate tasks, click **Stop and Save Logs** to capture the logging information to the appropriate log files.

The files are saved to the path that you designated in the Log Path field. The default log path is: c:\Program Files\Sophos\NAC\Support Tools\Logs. For information on the type of log files and what they contain, see [Log Files](#) on page 11.

Note: The Stop and Save Logs button is grayed out when logging is disabled.

3.1.1 Debug Logging Tab Fields and Descriptions

Diagnostic logging severely impacts system performance. It is highly recommended that you start logging, capture logging information, and immediately stop logging. Ideally, you should select only the necessary subsystems and avoid starting all logging.

Note: Logging is set at a maximum level and encompasses log error, warning, informational, full trace, and call stack messages.

Fields	Descriptions
Logging Type	
Flat File	Sets the logging to generate flat files. One flat file is created for each subsystem you select.
Event Log	Sets the logging to add subsystem information to the Event Log on the Sophos NAC server.
Logging Selections	
Log Path	Sets the path where the generated log files are placed.
RADIUS Enforcer	<p>Sets logging for the NAC RADIUS server. This selection is only used for DHCP enforcement.</p> <p>The NAC RADIUS server is the software component that checks Agent compliance results on behalf of the DHCP Enforcer.</p>
Policy Interface	<p>Sets logging for the Policy Interface service.</p> <p>The Policy Interface is the server-side component that retrieves policy for the Agent and verifies the validity of the Agent request.</p>
Definition Loader	<p>Sets logging for the definition loader.</p> <p>The definition loader is the server-side tool that is responsible for security application detection, signature version detection, scan engine version detection, last scan date detection, real-time protection detection, enabled detection, and auto-remediation actions.</p>

Fields	Descriptions
Registration Interface	Sets logging for the Registration Interface service. The Registration Interface is the server-side component that provides registration services to the Agent.
Reporting Interface	Sets logging for the Reporting Interface service. The Reporting Interface is the server-side component that accepts reporting data from the Agent. The Reporting Interface also verifies the the validity of the Agent request.
Policy Transfer	Sets logging for the Policy Transfer service. Policy Transfer is the component that transfers data from the policy data store to the report data store so that updated policy information is replicated in the reports.
All	Sets logging for all NAC subsystems.

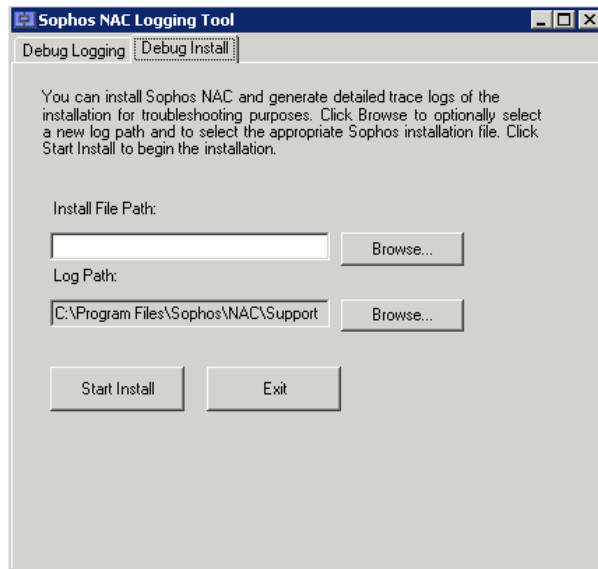
3.2 Sophos NAC Server Installation Logging

This tool should only be used to troubleshoot installation problems. You should first attempt to install Sophos NAC from the installation file. If you receive errors during the initial installation, you can use this tool to capture logging information about the installation.

1. Locate the Logging Tool on the Sophos NAC server. The default location of this tool is `c:\Program Files\Sophos\NAC\Support Tools`.
2. Double-click **LoggingUtil.exe**. The Logging Tool, Debug Logging tab displays.

3. Click the **Debug Install** tab.

The following window displays:



4. Select the appropriate path for the installation file you want to troubleshoot and the path where you want the log files to be placed, and then click **Start Install**.

For information about each field, see [Debug Install Tab Fields and Descriptions](#) on page 10.

Note: Once the installation is complete, the files are saved to the path that you designated in the **Log Path** field. The default log path is: c:\Program Files\Sophos\NAC\Support Tools\Logs. For information on the type of log files and what they contain, see [Log Files](#) on page 11.

3.2.1 Debug Install Tab Fields and Descriptions

Logging is set at a maximum level that is determined by Microsoft® Windows® Installer.

Fields	Descriptions
Install File Path	Selects the path to the installation file.
Log Path	Sets the path where the log files generated during the installation are placed.

3.3 Log Files

The default log file path is: c:\Program Files\Sophos\NAC\Support Tools\Logs on the Sophos NAC server. This path can be changed prior to generating the log files. Each time logging is started, any existing files in the specified path with the same name are overwritten.

Fields	Descriptions
AppEvent.xml	File that contains the exported application events from the Event Log on the Sophos NAC server. When the Event Log option is selected as the logging type, the subsystems log information is included in this file.
SystemEvent.xml	File that contains the exported system events from the Event Log on the on the Sophos NAC server. Internet Authentication Service (IAS) information is included in this log file.
Systeminfo.nfo	File that contains hardware and operating system information about the Sophos NAC server.
UserInfo.txt	File that contains account information, such as account name and permissions, for users logged on to the Sophos NAC server and the account information under which the installed subsystems are running.
<Subsystem>.xml	File that contains Sophos NAC subsystem logging information. When the Flat File option is selected as the logging type, the application server subsystems are each saved to a separate flat file, noted below: <ul style="list-style-type: none"> ■ Policy Interface: PolicyInterfaceLog.xml ■ Definition Loader: CurrentDefsLoaderLog.xml ■ Registration Interface: RegistrationInterfaceLog.xml ■ Reporting Interface: ReportingInterfaceLog.xml ■ Policy Transfer: PolicyTransferLog.xml
Install<datetime>.log	Microsoft Windows Installer output file that contains information about the installation. This file is generated for only the Debug Install tab functions.
SophosNACLogs.zip	File that includes all Debug Logging tab log files.
InstallLogs.zip	File that includes all Debug Install tab log files.

4 Maintenance Mode Tool

Use the Maintenance Mode tool when you upgrade Sophos NAC, perform database maintenance, and/or experience network problems or database issues. This tool is a command line tool used to turn maintenance mode on or off. The tool stops the appropriate Sophos NAC services so that you can perform required maintenance. Once you are ready to return to production, stop the Maintenance Mode tool. The tool automatically restarts the services that were stopped.

When Sophos NAC is in maintenance mode, the Sophos NAC Agent recognizes the mode and performs without error, interruption, or maintenance mode indication to users. The Agent saves all assessment and report information locally until the software returns to production mode. Also, the Agent continues assessing against the cached policy, and if Agent quarantine is being used, the endpoint can still be quarantined based on the rules in the cached policy. Additionally, if you are using DHCP enforcement, the DHCP Enforcer access templates and the exemptions are cached and all DHCP requests are responded to using the cached DHCP Enforcer access templates and exemptions.

4.1 Running the Maintenance Mode Tool

1. From a command prompt on the Sophos NAC server, go to the Program Files\Sophos\NAC\Support Tools directory.
2. Type `MaintMode.exe /start`. This command places Sophos NAC in maintenance mode.
3. Type `MaintMode.exe /stop`. This command returns Sophos NAC to production mode.

4.2 Maintenance Mode Tool Commands

The commands are not case-sensitive. Command parameters use forward slashes /, and then the parameter name. Any DOS parameter value that contains a space requires quotes.

Commands	Descriptions
MaintMode.exe /start	Starts the Maintenance Mode tool.
MaintMode.exe /stop	Stops the Maintenance Mode tool.
MaintMode.exe /E:silent	Specifies that no messages are written to the console. Error messages are always written to the Event Log.
MaintMode.exe /E:error	Specifies that only errors are written to the console. Error messages are always written to the Event Log.
MaintMode.exe /E:warn	Specifies that errors and warnings are written to the console. Error messages are always written to the Event Log.

Commands	Descriptions
MaintMode.exe /E:info	Specifies that errors, warnings, and informational messages are written to the console. Error messages are always written to the Event Log.
MaintMode.exe /?	Displays the Maintenance Mode tool Help window.

5 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.