

Sophos NAC Manager tools guide

Product version: 3.9

Document date: January 2012



Contents

- 1 About this guide.....3
- 2 Logging tool.....4
- 3 Maintenance Mode tool.....8
- 4 Technical support.....10
- 5 Legal notices.....11

1 About this guide

This guide is intended for users who have installed Sophos NAC Manager and want to use either the Logging tool or the Maintenance Mode tool.

The Logging tool enables you to turn on installation and subsystem logging to perform troubleshooting.

The Maintenance Mode tool can be used when you perform database maintenance, or experience network problems or database issues.

Sophos documentation is published at www.sophos.com/support/docs/.

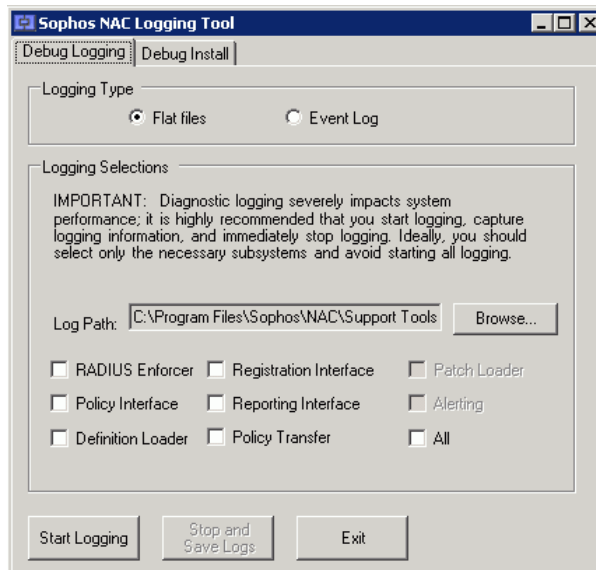
2 Logging tool

The Logging tool enables you to turn on installation and subsystem logging to perform 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: We recommend that you use this tool for troubleshooting purposes only when guided by a Sophos representative, and that you do not leave logging enabled since it can severely impact system performance.

2.1 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**.



3. On the **Debug Logging** tab, 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](#) (page 5).

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

4. Perform the appropriate tasks on the NAC Server for which you want to capture logging information.
5. Once you have performed the appropriate tasks, click **Stop and Save Logs** to save 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](#) (page 7).

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

2.2 Debug Logging tab fields and descriptions

Diagnostic logging severely impacts system performance. We highly recommend that you start logging, save logging information, and then 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 NAC Server.
Logging Selections	
Log Path	Sets the path where the generated log files are placed.
RADIUS Enforcer	Sets logging for the NAC Server. This selection is only used for DHCP enforcement. The NAC Server is the software component that checks Agent compliance results for the DHCP Enforcer.
Policy Interface	Sets logging for the Policy Interface service. The Policy Interface is the server-side component that retrieves policy for the Agent and verifies the validity of the Agent request.
Definition Loader	Sets logging for the definition loader. The definition loader is the server-side tool that is responsible for security application detection, signature version detection, scan engine version detection,

Fields	Descriptions
	last scan date detection, real-time protection detection, enabled detection, and auto-remediation actions.
Registration Interface	Sets logging for the Registration Interface service. The Registration Interface is the server-side component that provides registration services to the Agent. The Registration Interface performs a user authentication each time that the Agent registers for the first time or re-registers.
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 validity of the Agent request.
Policy Transfer	Sets logging for the Policy Transfer service. Policy Transfer is the server-side 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.

2.3 Sophos NAC Server installation logging

This tool should only be used to troubleshoot installation problems. You should first attempt to install Sophos NAC. 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**.
3. Click the **Debug Install** tab.
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](#) (page 6).

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](#) (page 7).

2.4 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.

2.5 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 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 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 NAC Server.
UserInfo.txt	File that contains account information, such as account name and permissions, for users logged on to the 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 Sophos NAC 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
SophosNACLogs.zip	File that includes all Debug Logging tab log files.
InstallLogs.zip	File that includes all Debug Install tab log files.

3 Maintenance Mode tool

Use the Maintenance Mode tool when you 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 Compliance 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.

Note: You do not need to use this tool during a Sophos NAC upgrade. The installation puts the NAC Server in maintenance mode and takes the server out of maintenance mode when the installation completes.

3.1 Running the Maintenance Mode tool

1. From a command prompt on the Sophos NAC Server, go to the C:\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.

3.2 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 command line dialog box. 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.

Commands	Descriptions
MaintMode.exe /E:warn	Specifies that errors and warnings are written to the console. Error messages are always written to the Event Log.
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.

4 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>.
- Download the product documentation at <http://www.sophos.com/support/docs/>.
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

5 Legal notices

Copyright © 2012 Sophos Limited. 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 license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.