

SOPHOS

Sophos NAC Advanced tools guide

Product version: 3.2

Document date: March 2011



Contents

1 About This Document.....	3
2 Loader Tool.....	4
3 Authentication Test Tool.....	7
4 Logging Tool.....	10
5 Secret Encryption Tool.....	15
6 Maintenance Mode Tool.....	17
7 Technical Support.....	19
8 Legal Notices.....	20

1 About This Document

This document contains information about the following for Sophos NAC Advanced:

- Loader Tool
- Authentication Test Tool
- Logging Tool
- Secret Encryption Tool
- Maintenance Mode Tool

1.1 Intended audience

The intended audience for this documentation is an IT generalist for a small- to medium-sized business. The audience may include IT specialists for businesses with more than 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 enables administrators to import new and updated applications and application types to their Sophos Compliance Databases. This tool is installed as part of the Sophos Compliance Application Server.

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. We recommend 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 Compliance Application 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.

4. Repeat steps 1-3 on all additional Compliance Application Servers.

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 Compliance Application Server.

- 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.
- Repeat steps 1-3 on additional Compliance Application Servers.

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
Loader /A:export /B:application /I:id /F:export.xml	Exports an application by unique ID. The application definition is saved in the XML file specified.
Loader /A:export /B:application /N:"name" /F:export.xml	Exports an application by name. The application definition is saved in the XML file specified.
Loader /A:export /B:application /n:* /F:export.xml	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 Compliance Databases, export applications from the Compliance 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 Authentication Test Tool

The Authentication Test tool enables you to troubleshoot authentication issues with the RADIUS Enforcer. You can use the Authentication Test tool to view data in the RADIUS packets. The Authentication Test tool also emulates the way the Registration Policy Interface, VPN concentrator, or 802.1x switch views and sends data in the RADIUS packets. This tool generates the same behavior as the RADIUS Enforcer and gives you more diagnostic information for troubleshooting.

3.1 Using the Authentication Test Tool

1. Locate the Authentication Test tool.

The default location of this tool is C:\Program Files\Sophos\NAC\Support Tools.

2. Double-click **Auth Test.exe**.

The following window displays:

The screenshot shows the 'Auth Test' application window. The window title is 'Auth Test'. It features a 'Results:' area on the right with a 'Copy' button. The main area contains several sections: 'User Name' and 'Password' (with a 'Mask' checkbox), 'Shared Secret', 'Login Type' (radio buttons for Agent (Group), Compliance, Admin), 'Authentication Method' (radio buttons for PAP (SecurId, LDAP), MS-CHAP v1, CHAP, MS-CHAP v2), and 'RADIUS Settings' (Server: localhost, Port: 1645, Timeout (sec): 10, Attempts: 1). At the bottom are 'Run Test' and 'Close' buttons.

Note: The Shared Secret field is automatically populated with the shared secret that was created during the Sophos NAC Advanced installation. If the shared secret does not display and you do not know it, you can use the Secret Encryption tool to view the Shared Secret. For more information see, [Viewing the RADIUS Shared Secret](#) (page 15).

3. Type the appropriate information in the available fields, and then click **Run Test**.

The results of the test display in the Results area. For information about each field, see [Fields and Descriptions](#) (page 8).

Note: All fields are required. Use the Copy button to copy the results to the Clipboard. You can then paste the results into a program of your choice.

3.2 Fields and Descriptions

Fields	Descriptions
User Name	The user name that is used to access the RADIUS server. The value is sent just as it is typed to the RADIUS server; therefore, it must be exact.
Password	The password that is used to access the RADIUS server.
Mask	When the Mask check box is selected, the password field displays with **** symbols.
Shared Secret	This field specifies the shared secret of the RADIUS server that you want to use for troubleshooting.
Login Type	The login type determines the authentication testing method. The following option buttons are available: <ul style="list-style-type: none"> ■ Agent: When the Agent option button is selected, authentication and user group lookup are tested for the user name and password in the User Name and Password fields. The user group information displays as part of the results. This option button is selected by default. ■ Compliance: When the Compliance option button is selected, authentication and compliance are tested for the user name and password in the User Name and Password fields. ■ Admin: When the Admin option button is selected, authentication for the user name and password typed in the User Name and Password fields are tested. Compliance and group lookup are not tested.
Authentication Method	The authentication method specifies the authentication method such as PAP, CHAP, MS-CHAP V.1, and MS-CHAP V.2. MS-CHAP V.2 is the default setting.
Server IP	The server IP specifies the IP address or host name of the RADIUS server.
Port	The port specifies the port for the UDP RADIUS request. The default is 1645. Another commonly used port is 1812.

Fields	Descriptions
Timeout (sec)	The timeout specifies the length of time the Authentication Test tool waits for a response from the RADIUS server. The default is 10 seconds.
Attempts	This number specifies the maximum number of requests the Authentication Test tool will make until a valid response is received from the RADIUS server. The default is 1.
Results	The Results area displays the results of the test.

4 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: We recommend 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.

4.1 Sophos NAC Advanced Subsystem Logging

1. Locate the Logging Tool on the Sophos Compliance Application Server or RADIUS 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](#) (page 10).

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 the appropriate tasks on the Sophos Compliance Application Server or RADIUS server for which you want to capture logging information.
5. 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](#) (page 13).

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

4.1.1 Debug Logging Tab Fields and Descriptions

Diagnostic logging severely impacts system performance. We strongly recommend 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 Compliance Application Server.
Logging Selections	
Log Path	Sets the path where the generated log files are placed.
RADIUS Enforcer	<p>Sets logging for the Compliance RADIUS Server.</p> <p>The RADIUS Enforcer is the software component that checks Agent compliance results by acting as a proxy to perform authentication protocol mapping, and enforces appropriate network access for and any device that supports RADIUS authorization. The RADIUS Enforcer translates Agent authentication requests into RADIUS commands and communicates with the appropriate user store to authenticate the user, obtain the user group membership, and permit, deny, or quarantine network access as appropriate.</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>
Registration Interface	<p>Sets logging for the Registration Interface service.</p> <p>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.</p>
Reporting Interface	<p>Sets logging for the Reporting Interface service.</p> <p>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.</p>
Policy Transfer	<p>Sets logging for the Policy Transfer service.</p> <p>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.</p>

Fields	Descriptions
Patch Loader	<p>Sets logging for the OS patch loader.</p> <p>The OS patch loader is the server-side tool that is responsible for adding and updating OS patches to be included into policy using the Sophos Compliance Manager. The tool is scheduled to run each night by default and pulls the OS patches CAB file from the Compliance Application Server to ensure up-to-date patch information.</p>
Alerting	<p>Sets logging for the Compliance Application Server Alerting service.</p> <p>The Alerting service processes alertable events (i.e., new compliance data reported or enforcement actions taken), and based on the alert definitions generates alert actions (Event Log or e-mail) if the defined criteria and thresholds have been met.</p>
All	<p>Sets logging for all Sophos NAC Advanced subsystems. This setting also includes logging for the RADIUS Enforcer that is installed on the Compliance Application Server.</p>

4.2 Sophos NAC Advanced Installation Logging

This tool should only be used to troubleshoot installation problems. You should first attempt to install Sophos NAC Advanced 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 Compliance Application 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.
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 12).

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 13).

4.2.1 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.

4.3 Log Files

The default log file path is: C:\Program Files\Sophos\NAC\Support Tools\Logs on the Sophos Compliance Application 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 Compliance Application Server. When the Event Log option is selected as the logging type, the subsystems log information is included in this file. The RADIUS Enforcer logging information, for the RADIUS Enforcer installed on the Compliance Application Server, is always included in this file, regardless of the logging type selected.
SystemEvent.xml	File that contains the exported system events from the Event Log on the Sophos Compliance Application 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 Compliance Application Server.
UserInfo.txt	File that contains account information, such as account name and permissions, for users logged on to the Sophos Compliance Application Server and the account information under which the installed subsystems are running.
<Subsystem>.xml	File that contains Sophos NAC Advanced subsystem logging information. When the Flat File option is selected as the logging type, the Compliance 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

Fields	Descriptions
	<ul style="list-style-type: none">■ Patch Loader: PatchLoaderLog.xml■ Alerting: AlertingLog.xml <p>Note: The RADIUS Enforcer subsystem logging information is always included in the AppEvent.xml file, regardless of the logging type selected.</p>
Install<datetime>.log	<p>Microsoft Windows Installer output file that contains information about the installation.</p> <p>This file is generated for only the Debug Install tab functions.</p>
SophosNACLogs.zip	<p>File that includes all Debug Logging tab log files.</p>
InstallLogs.zip	<p>File that includes all Debug Install tab log files.</p>

5 Secret Encryption Tool

Use the Secret Encryption tool to change the RADIUS shared secret. The RADIUS shared secret is specified and encrypted during the Sophos NAC Advanced installation. The Secret Encryption tool is run from a command prompt and resides in the C:\Program Files\Sophos\NAC\Support Tools folder on the Sophos Compliance Application Server.

Note: The Sophos NAC Advanced Registration Interface, the web.config file, and the Internet Authentication Service (IAS) on the Compliance Application Server use the RADIUS shared secret.

5.1 Viewing the RADIUS Shared Secret

1. From a command prompt on the Sophos Compliance Application Server, go to the C:\Program Files\Sophos\NAC\Support Tools directory.
2. To view the RADIUS shared secret, type **SecretEncryptionTool.exe /View**.

5.2 Changing the RADIUS Shared Secret

1. From a command prompt on the Sophos Compliance Application Server, go to the C:\Program Files\Sophos\NAC\Support Tools directory.
2. To change the RADIUS shared secret, type **SecretEncryptionTool.exe /Set /Secret=<shared secret>**.
3. Repeat steps 1-2 on all Sophos Compliance Application Servers.

5.3 Secret Encryption 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
SecretEncryptionTool.exe /ViewSecret	Displays the RADIUS shared secret used by the Registration interface, Compliance Manager, and Internet Authentication Service (IAS).
SecretEncryptionTool.exe /Set	Changes the RADIUS shared secret used by the Registration interface, Compliance Manager, and Internet Authentication Service (IAS). Note: This command is used with the /Secret command.

Commands	Descriptions
SecretEncryptionTool.exe /Set /Secret=<shared secret>	Changes the RADIUS shared secret used by the Registration interface, Compliance Manager, and Internet Authentication Service (IAS).
SecretEncryptionTool.exe /?	Displays the Secret Encryption tool Help window.

6 Maintenance Mode Tool

Use the Maintenance Mode tool when you upgrade Sophos NAC Advanced, 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 Advanced 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 Advanced 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.

6.1 Running the Maintenance Mode Tool

1. From a command prompt on the Sophos Compliance Application Server, go to the C:\Program Files\Sophos\NAC\Support Tools directory.
2. Type **MaintMode.exe /start**. This command places Sophos NAC Advanced in maintenance mode.

Note: You must repeat this step on all Sophos Compliance Application Servers.

3. Type **MaintMode.exe /stop**. This command returns Sophos NAC Advanced to production mode.

Note: You must repeat this step on all Sophos Compliance Application Servers.

6.2 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.

Commands	Descriptions
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.
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.

7 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.

8 Legal Notices

Copyright © 2011 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 licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.