

SOPHOS

Sophos Compliance Agent configuration guide

Product version: 3.3

Document date: September 2009



Contents

1 About this guide.....	3
2 Quarantine Agent.....	5
3 Dissolvable Agent.....	12
4 Agent languages.....	16
5 Technical support.....	17
6 Copyright.....	18

1 About this guide

This guide describes Compliance Agent configuration for Sophos Endpoint Security and Control software.

In particular, it provides information on:

- Design, configuration, and logging for the Compliance Agent and Dissolvable Compliance Agent.
- Interface components for each Agent, such as dialog boxes.
- Supported Agent languages.

This guide is for you if:

- You are using Enterprise Console.
- You are using Sophos NAC for Endpoint Security and Control.
- You want information about how the Compliance Agent and Compliance Dissolvable Agent are designed.
- You want to know what interface components display on the endpoint.

See the *Sophos Endpoint Security and Control quick startup guide* prior to reviewing this guide.

All Sophos Endpoint Security and Control documents are available at:

http://www.sophos.com/support/docs/Endpoint_Security_Control-all.html.

1.1 Overview

The Sophos Compliance Agent is a configurable endpoint application that assesses and enforces compliance with NAC policies. The Agent retrieves the NAC policy, assesses the endpoint for compliance, can automatically remediate applications and provide user messages, and submits reporting information.

Sophos NAC supports two Agent configurations. Enterprises can install the Quarantine Agent on an endpoint running Microsoft® Windows®. The Dissolvable Agent is designed for guest users running Microsoft Windows.

- **Quarantine Agent:** The Quarantine Agent assesses endpoints to determine whether they are compliant with the NAC policy. Assessments are performed prior to and periodically after network access is permitted. The Agent requires little or no user interaction. The Quarantine Agent has a quarantine feature that provides enforcement and limits endpoints to specific areas of the network when they are not compliant with the NAC policy.
- **Dissolvable Agent:** The Dissolvable Agent assesses endpoints to determine whether they are compliant with the NAC policy prior to permitting network access. The Dissolvable Agent must run from a browser. The Dissolvable Agent is designed for users who do not or cannot have an Agent installed on the endpoint, yet who must still access specific network resources,

such as contractors or guests. The Dissolvable Agent has no enforcement capabilities itself, but can be used with DHCP enforcement.

For more information on DHCP enforcement, see the *Sophos NAC DHCP configuration guide*.

2 Quarantine Agent

This section contains design and configuration information about the Quarantine Agent.

2.1 Design

The Quarantine Agent is a system tray application that is installed on the endpoint and performs processing operations on a periodic basis in accordance with the NAC policy defined in the NAC Manager. The Quarantine Agent requires local administrator privileges to be installed on the endpoint.

Agent settings

The Quarantine Agent visually displays as an icon in the system tray, which conveys the Agent's current state. The Quarantine Agent icon changes to indicate when the endpoint is in quarantine, when it has full network access, or when results are pending. Agent settings, which are configured in the NAC Manager in Agent configuration templates, can be used to control display options and functionality of the interface. Once an Agent configuration template is added to a policy, Agents can retrieve the policy and implement the settings on the endpoint.

Processing operations

The Quarantine Agent runs an initial compliance assessment and then periodically runs compliance assessment operations to ensure that the endpoint remains compliant with the NAC policy. The Quarantine Agent performs all operations - retrieve policy, assess policy, enforce policy, remediate, and report - even if one of the operations fails. If an operation fails, it is retried the next time the operation is scheduled to occur.

Network access

The user is assigned network access based on the endpoint's compliance or access state and the associated network access templates also defined in the policy. For example, if the endpoint is not compliant, the Agent can quarantine the endpoint and the endpoint's network access can be restricted as defined by associated non-compliant access templates. If access is restricted, the Agent must enable users to remediate in order to regain full network access and must also enable access to a proxy server for remediation if one is being used.

Proxy server access

If user authentication through a proxy server is required for the Agent to communicate with the NAC Server, the Credential Request dialog box displays on the endpoint to prompt the user for a username and password prior to the policy being retrieved. If you have saved the proxy username and password as Agent settings in the NAC Manager, the Agent automatically manages subsequent endpoint authentication requests without prompting the user again.

Quarantine and compliance assessments

An endpoint remains in quarantine until compliance to the policy is met. However, users can override the quarantine during an Agent session if the NAC policy permits it. The quarantine is reset when the user disables the quarantine override or when the user logs off the machine. In addition to continuous compliance assessments, users can re-assess their endpoint compliance

status at any time using either the Check Compliance menu option associated with the Quarantine Agent system tray icon or the Check Compliance button on the Results dialog box.

Reporting and messaging

Report data includes information on software applications installed or not installed on the endpoint, the endpoint compliance state when assessed against the NAC policy, and messages displayed to the user or actions performed on the endpoint. During operation, the Quarantine Agent displays user messages, which are defined in the NAC Manager, and errors in operation to the user.

2.2 Configuration

To configure the Quarantine Agent, perform the following steps:

1. **In the NAC Manager, create network resources and apply them to the Agent Enforcer access templates used in policy for non-compliant endpoints.**

Network resources are applications or devices that are required for endpoint remediation or those that quarantined endpoints should be denied access to. The Agent Enforcer access templates are used in association with policy to identify the network resources that endpoints can or cannot access when using the Quarantine Agent for enforcement. The network resources should be available to a quarantined endpoint for remediation purposes, as well as provide access to a proxy server for remediation if one is being used.

2. **Deploy the Sophos Compliance Agent to endpoints, using Sophos Enterprise Console.**

Using the Sophos Enterprise Console Protect computers wizard, the Quarantine Agent is deployed to endpoints. After the Agent is deployed, the endpoint retrieves its assigned policy, and settings defined in the policy are implemented. The policy that is associated with the endpoint's group in Sophos Enterprise Console is the one retrieved by the Agent and used for the endpoint's compliance assessment.

For more information on network resources, Agent Enforcer access templates, and policies, see the NAC Manager help.

2.3 Logging

For troubleshooting purposes, the Quarantine Agent supports multiple log files that are saved to the endpoint's hard disk.

The Sophos Compliance 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**.

Additionally, logging can be used to troubleshoot Agent activity on the endpoint. Logging affects the Quarantine Agent's performance; therefore, logging should be enabled only for troubleshooting purposes and it should be disabled after troubleshooting is complete. Log files exclude user-sensitive

data and contain customizable levels of information. Logging is enabled from the Agent's About dialog box and the logging level is customizable as an Agent setting.

The three log files are:

- **Session Log:** Provides high-level error information.
- **Trace Log:** Provides detailed error information.
- **Agent Log:** Provides error information that pertains to the Agent application.

1. In the NAC Manager, access the **Create Agent Configuration Template** page.
2. Add the **Logging** Agent setting to the Agent configuration template, and then select the appropriate logging level.

For more information on Agent settings, see the NAC Manager help.

3. On the endpoint, open the Agent's **About** dialog box, and select the **Enable Logging** check box.

Log files are located in the `<drive>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Logs` folder or, for Vista, in the `<drive>:\ProgramData\Sophos\Sophos NAC\Logs` folder.

4. When troubleshooting is complete, on the endpoint, open the Agent's **About** dialog box, and clear the **Enable Logging** check box.

2.4 Icons, menus, balloons, and dialog boxes

The following section contains details about available Quarantine Agent system tray icons, tooltips, menu options, balloons, and dialog boxes.

2.4.1 System tray icons and tooltips

The system tray icons convey the current state of the Agent in the following ways:

- The tray icons show the Agent's various states.
- Hovering over the tray icon displays the tooltip associated with the icon.

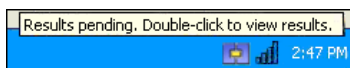





Figure 1: System tray icon and tooltip example

The following table provides icon information.

Icon	Tooltip text	Description
	Results pending. Double-click to view results.	Icon that displays when actions are pending and are displayed in the Results dialog box.
	Sophos Compliance Agent - Idle. Machine in quarantine.	Icon that displays when the endpoint is in quarantine.
	Sophos Compliance Agent - Idle.	Icon that displays when the Agent is idle.

2.4.2 Menu options

The Agent menu provides access to available Agent actions by right-clicking the system tray icon. Double-clicking the tray icon performs the Show Results default menu action (displayed in bold in the example).

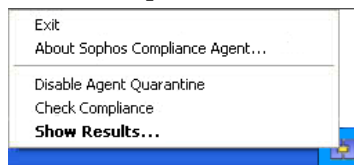


Figure 2: Menu example

The following table identifies the menu text and descriptions.

Menu text	Description
Exit	Exits the Agent, removes the icon from the system tray, and places the endpoint in quarantine, if applicable. Note: If the Show Exit Agent setting is Show, this menu option displays. If the Show Exit Agent setting is Hide (default value), this menu option does not display. For more information on Agent settings, see the NAC Manager help.
About Sophos Compliance Agent...	Displays the About dialog box.
Disable Agent Quarantine	Overrides the endpoint quarantine. When quarantine is disabled, a check mark displays next to the text. When quarantine is enabled, a check mark does not display next to the text.

Menu text	Description
	Note: If the Quarantine Override option in the policy is set to False (i.e. the endpoint is not allowed to override the quarantine), this menu option does not display.
Check Compliance	Begins a user-initiated compliance check that includes the retrieve policy, assess policy, enforce policy, remediate, and report operations.
Show Results...	Displays the Results dialog box with messages from the most recent compliance assessment.

2.4.3 Balloons

The balloons provide additional textual information regarding actions by or required for the Agent. The balloon can display if a user's actions are required, such as results are pending, or if the Agent state changes.

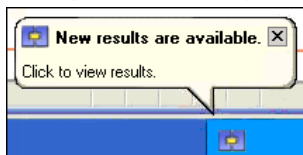





Figure 3: Balloon example

The following table identifies the associated icon, balloon text, and descriptions.

Icon	Balloon text	Description
	Caption: New results are available. Text: Click to view results.	Balloon when actions are pending and are displayed in the Results dialog box.
	Caption: Your machine has been placed in quarantine. No default text.	Balloon when the endpoint is in quarantine.
	Caption: Your machine has been removed from quarantine. No default text.	Balloon when the endpoint has been removed from quarantine.

2.4.4 Credential Request dialog box

The Credential Request dialog box displays if authentication through a proxy server is required for the Agent to communicate with the NAC Server.

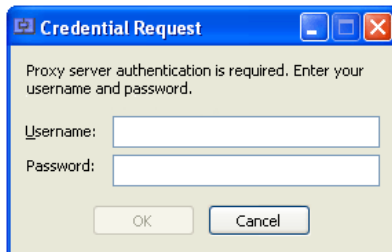


Figure 4: Credential Request dialog box example

2.4.5 Results dialog box

The Results dialog box displays any policy-defined user messages or error messages available to the user. The Results dialog box is available from the Show Results option on the menu and displays the messages from the latest compliance assessment.

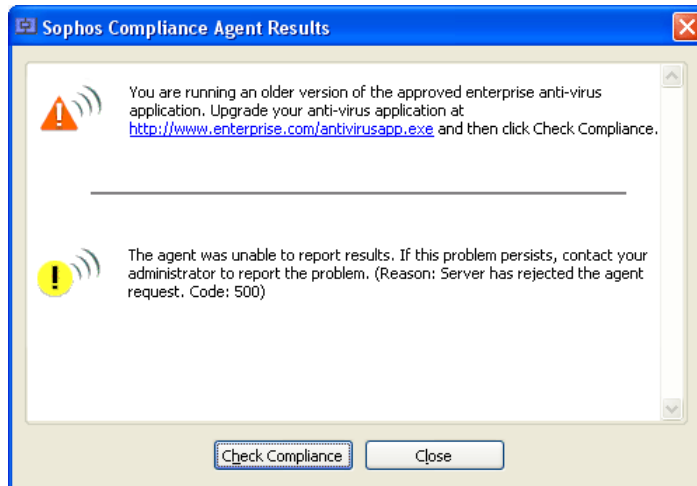


Figure 5: Results dialog box example

2.4.6 About dialog box

The About dialog box displays Agent information, copyright information, and the Enable Logging check box. The About dialog box is available from the About option on the menu.



Figure 6: About dialog box example

3 Dissolvable Agent

This section contains design and configuration information about the Dissolvable Agent.

3.1 Design

The Dissolvable Agent can be installed on any Windows-based web server, including the NAC Server, and provides an accessible web page that permits guest users to run the Dissolvable Agent. The Dissolvable Agent is a standalone application that runs locally on the endpoint and does not require administrator or power user privileges to run. If user authentication through a proxy server is required for the Dissolvable Agent to communicate with the NAC Server, the Web browser prompts the user for a username and password.

Processing operations

Once started, the Dissolvable Agent displays a series of dialog boxes that indicate progress and actions as necessary. The Dissolvable Agent performs the processing operations - retrieve policy, assess policy, enforce policy, remediate, and report - each time it is invoked in accordance with the NAC policy defined in the NAC Manager. When the processing operations are complete, the Dissolvable Agent removes itself from the endpoint. The Dissolvable Agent has no enforcement capabilities itself, but can be used with DHCP enforcement.

Reporting and messaging

Report data includes information on software applications installed or not installed on the endpoint, the endpoint compliance state when assessed against the NAC policy, and messages displayed to the endpoint user. During operation, the Dissolvable Agent displays user messages, which are defined in the NAC Manager, and errors in operation to the user.

3.2 Configuration

To use the Dissolvable Agent, you must first install it on a Windows-based web server that is accessible to guest users. The Dissolvable Agent may be installed on the same server as Sophos NAC.

1. **Install the Sophos Compliance Dissolvable Agent on a Windows-based web server.**

The Dissolvable Agent is available from the Sophos web site. Alternatively, you can install the Dissolvable Agent from the Sophos Install CD. The Sophos Compliance Dissolvable Agent installation installs all of the files that support the Dissolvable Agent. For more information, see the *Sophos Endpoint Security and Control advanced startup guide*.

2. **Distribute the Sophos Compliance Dissolvable Agent URL to guest users, as necessary.**

The endpoint retrieves its assigned policy and assesses the endpoint for compliance. If you install the Dissolvable Agent to the default directory, endpoints can access the Dissolvable Agent using the following URL: `http://<ip address/DNS name>/dissolvableagent`. The IP address or DNS name is the web server where you installed the Dissolvable Agent.

3.3 Logging

There are no settings that are defined in the NAC Manager for the Dissolvable Agent. The logging setting is defined on the endpoint.

For troubleshooting purposes, the Dissolvable Agent supports multiple log files that, if used, are saved to the endpoint's hard disk. Logging affects the Dissolvable Agent's performance; therefore, logging, which can be enabled from the About dialog box, should be enabled only for troubleshooting purposes and it should be disabled after troubleshooting is complete. Log files exclude user-sensitive data and contain customizable levels of information.

The three log files are:

- **Session Log:** Provides high-level error information.
- **Trace Log:** Provides detailed error information.
- **Agent Log:** Provides error information that pertains to the Agent application.

1. Start the Dissolvable Agent.
2. Click the Sophos NAC icon on the **Results** dialog box and select **About Sophos Compliance Agent**.
3. In the **About** dialog box, select the **Enable Logging** check box.
4. Run the Dissolvable Agent.
5. Locate the log files, which can be found in the `<drive>:\Sophos\SDA<random number>\Logs` directory.
6. When troubleshooting is complete, run the Dissolvable Agent again, access the Dissolvable Agent's **About** dialog box, and clear the **Enable Logging** check box.

3.4 Dialog boxes

The following section contains details about available Dissolvable Agent dialog boxes.

3.4.1 Credential Request dialog box

The Credential Request dialog box displays if authentication by a proxy server is required for the Dissolvable Agent to communicate with the NAC Server.

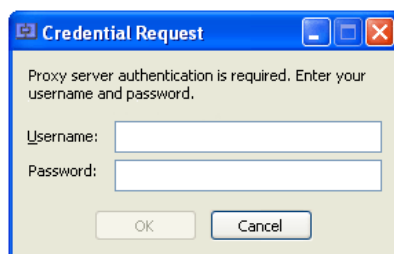


Figure 7: Credential Request dialog box example

3.4.2 Progress dialog box

The Progress dialog box displays while the Agent is performing the processing operations: retrieve policy, assess policy, enforce policy, remediate, and report. The Progress dialog box displays the status text, step-by-step operations progress, and overall operations progress.

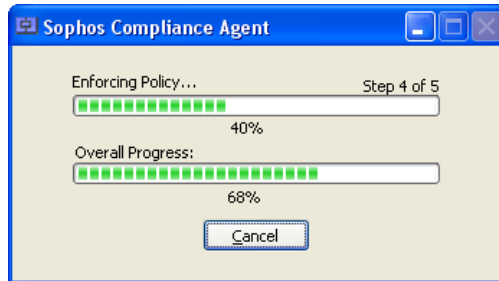


Figure 8: Progress dialog box example

3.4.3 Results dialog box

The Results dialog box displays any policy-defined user messages or error messages available to the user.

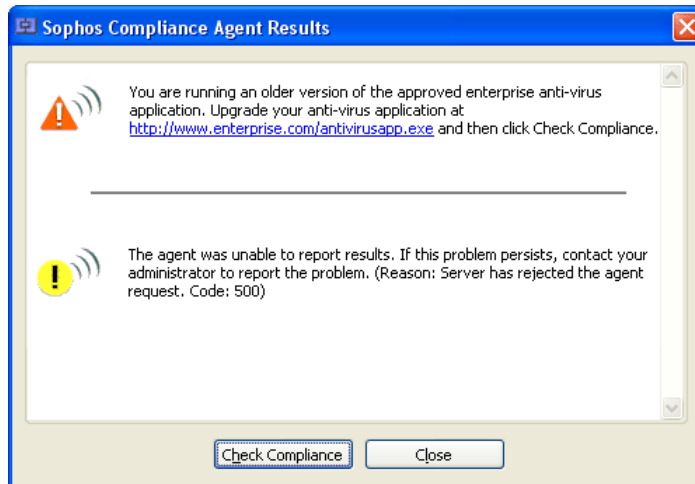


Figure 9: Results dialog box example

3.4.4 About dialog box

The About dialog box displays Agent information, copyright information, and the Enable Logging check box. The About dialog box is available by clicking the Sophos icon on the Results dialog box.



Figure 10: About dialog box example

4 Agent languages

The Agent supports the following eight languages by default: English, French, Spanish, German, Italian, Japanese, Simplified Chinese, and Traditional Chinese.

User messages are defined in profiles in the NAC Manager. The Agent displays user messages in a specific language only if they are defined.

Sophos recommends that you create a message for a profile in English (default language) so that, if a message of another language cannot be displayed, a message always displays to the endpoint user.

For more information on creating user messages, see the NAC Manager help.

5 Technical support

For technical support, visit <http://www.sophos.com/support>.

If you contact technical support, provide as much information as possible, including the following:

- Sophos software version number(s)
- Operating system(s) and patch level(s)
- The exact text of any error messages

6 Copyright

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.