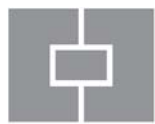


SOPHOS



sophos **nac**

ADVANCED

Agent Profile



Copyright © 2011 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in 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 are trademarks or registered trademarks of their respective owners.

Document version 3.2
Published January 2011

Table of Contents

Agent Descriptions	4
Agent Architecture Overview	4
Resource Utilization.....	4
Network Bandwidth.....	5
Secure Execution.....	7
Memory Consumption	7
Agent Required User Permissions	8

Agent Descriptions

Prior to installation, you must configure the Sophos Compliance Agent to use one of the following options:

- **Quarantine Agent:** The Quarantine Agent assesses and verifies compliance with corporate security policy prior to gaining access to network resources and on a periodic basis during the endpoint's session, requiring little or no user interaction. The Quarantine Agent is also equipped with a quarantine feature that provides client-side enforcement of endpoints that are not compliant with the corporate security policy; therefore, during compliance assessment, the Quarantine Agent also limits the endpoint to quarantined areas of the corporate network if the endpoint falls out of compliance with policy. The Quarantine Agent is available to both remote and LAN users and can be used with additional enforcement types, such as RADIUS, DHCP, or 802.1x. Additionally, the Quarantine Agent can be integrated with third-party network access applications.
- **Continuous Agent:** The Continuous Agent assesses and verifies compliance with corporate security policy prior to gaining access to network resources and on a periodic basis during the endpoint's session, requiring little or no user interaction. The Continuous Agent shares all features of the Quarantine Agent without the quarantine feature. The Continuous Agent is available to both remote and LAN users who are using another enforcement type other than quarantine-based enforcement or in the case that enforcement is not an enterprise requirement. If enforcement is required for Continuous Agent users, another enforcement type, such as RADIUS, DHCP, or 802.1x, must be implemented. Additionally, the Continuous Agent can be integrated with third-party network access applications.

Note: The Continuous Agent is no longer supported in NAC version 3.2.6. The Quarantine Agent is recommended as the replacement for this agent.

- **Dissolvable Agent:** The Dissolvable Agent assesses and verifies compliance with corporate security policy prior to gaining access to network resources. The Dissolvable Agent must be downloaded to the endpoint using 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 RADIUS, DHCP, or 802.1x enforcement.

Agent Architecture Overview

The Compliance Agent is designed to assess, communicate, and report compliance to the Sophos Compliance Application Server in an accurate and efficient manner. The Agent architecture enables this efficiency by optimizing across four main areas that are of concern to administrators:

- Minimal disk footprint
- Minimal resource utilization
- Minimal network bandwidth
- Secure execution

Resource Utilization

Both the Quarantine and Continuous Agent configurations are driven by a small background process on the endpoint. The Agent does not remain active while continually polling for compliance; instead, it is event-driven. The Agent only becomes active when instructed by its timer to retrieve policy, assess policy, or report compliance. The timer intervals are configurable and specified in policy so that assessments can run frequently enough to ensure compliance. The assessment action is what uses the most system resources.

Network Bandwidth

Data transfer between the Compliance Agent and the Compliance Application Server is sporadic, not continuous. There are three events under which this data transfer occurs:

- **Policy Retrieval:** The Agent requests the current policy. If the local policy is current, no policy is downloaded.
- **Compliance Reporting:** The Agent periodically sends assessment results to the Compliance Application Server based on the assessment timer. This information is also added to the report data store. This reporting interval is configurable and can be specified per policy.
- **Reporting:** The Agent sends global reports during Agent registration. There is a direct correlation between the size of the policy and the size of the report; therefore, if the policy is very large, the report will also become large.

Average Bandwidth Generated per Profile

- **Patch:** If any patches are added to policy, then it will force the Agent to download the patch file, which is 1.7MB. Each patch that is added to policy after that will generate an average of .68KB.
- **Anti-Virus:** Each anti-virus profile that is added to policy generates an average of 5.7KB.
- **Firewall:** Each firewall profile that is added to policy generates an average of 1.81KB.

Agent bandwidth usage breakdown:

The following chart was based upon a policy with the following features: 25 Patches, 1 Sophos Assessment Application, 1 Sophos Anti-virus Profile.

Agent Functions	Size (KB)	Constant/Changing	Interval Used
Registration	6.3	Constant	Registration
Retrieve Policy	25.1	Changing (based on policy)	Policy Refresh
Patch Definitions	1,743.3	Changing (based on version of Shavlik)*	New Policy/Reboot/24hrs
Report (Set Compliance, Batch Create Agent Session, Batch Create Session Response)	17.16	Changing (based on policy)	Report

* The patch definitions file is pulled onto the Compliance Application Server nightly. When a new policy is created or an existing policy is updated, the Agent is forced to download the new patch file from the Compliance Application Server (based on policy): The bandwidth usage decreases if a smaller policy is used and increases if a larger policy is used.

Initial registration of Agent should generate the following actions:

Registration	6.3KB
Fetch Policy (based on policy)	25.1KB (based on policy size)
Patch Definitions	1743.3KB
Report (based on policy)	17.1KB

Total:	1791.8KB

Each new or updated policy should generate the following actions based on Policy Refresh Interval:

Fetch Policy: New 17.3KB (based on policy size)
 Patch Definitions 488.9KB (if Windows patches are in the policy)

Total: 506.2KB

Each login should generate the following actions:

Fetch Policy (based on policy) 25.1KB (based on policy size)
 Patch Definitions 1743.3KB
 Report (based on policy) 17.1KB

Total: 1785.5.8KB

Network Performance

The Quarantine Agent configuration inspects network packets coming from the endpoint to ensure the destination is valid according to the current assessment state and policy. To measure the effect on network performance, a series of FTP downloads was performed on 10MB and 75MB files from a local network address. Average download time for endpoints, both with and without the Quarantine Agent configuration installed, are noted in the following table:

Agent	10MB file (seconds)	75MB file (seconds)
No Agent Installed	12.5	81.3
Quarantine Agent Installed	14.2	83.7

As the test indicates, overall network performance is only slightly affected due to the filter driver that is installed with the Agent.

Agent Disk Space Utilization

The Compliance Agent consists mainly of 3 executables (AgentAPI, AgntTray, and AgntAsst), which combined are a total of 10.5MB of disk space in the Sophos installation directory. The following example includes a Quarantine Agent retrieving a policy that includes an Agent application, a firewall application, an anti-virus application, a service pack, and 50 patches. The following files were placed on the endpoint during the initial policy retrieval and assessment.

File	Size (KB)
Policy cache	134
Patch Assessment results	36
Other Policy results	54
Report	225

The encrypted report file is stored on the endpoint until the report interval, which is specified in policy, is reached. When this report interval is reached, the report file is sent to the Compliance Application Server for reporting, and the file is deleted from the endpoint. This report file grows by only a miniscule amount as long as the state of the endpoint remains unchanged.

Also, the policy cache is stored in an encrypted format on the endpoint. This file size may increase or decrease after a policy refresh if the corresponding policy on the Compliance Application Server changes.

Secure Execution

The Compliance Agent does not require local administrator privileges to execute on the endpoint and operates normally in restricted user mode. This feature allows IT administrators to lock down endpoints to further secure vital corporate assets.

Memory Consumption

Separate tests using the Quarantine and Dissolvable Agent configurations on Windows® XP SP3 determined the Agent memory consumption. The following measurements for average private bytes and average working set are for a period of 5 minutes. Private bytes measure the current size, in bytes, of memory that a process has allocated that cannot be shared with other processes. Working set measures the current size, in bytes, of the set of memory pages recently touched by the threads in the process. These two measurements serve as an indication of the memory consumption of the two Agent services. For all policies in these tests, the Policy Refresh Interval and the Report Interval were specified as 5 minutes, the Assess and Enforce Interval was specified as 5 minutes. The Agent was monitored when the policy assessment began until it ended as this is the time when the Agent will be using the most resources. All results are in megabytes.

Small Policy: OS-Win XP, 35 Patches, 1 NAC Agent Assessment, 1 Firewall

Medium Policy: OS-Win XP, 55 Patches, 1 NAC Agent Assessment, 1 Firewall, 1 Anti-Virus

Large Policy: OS-Win XP, 75 Patches, 1 NAC Agent Assessment, 1 Firewall, 1 Anti-Virus, 1 Anti-Spyware

Test	Agent Configuration	Service	Avg. Private Bytes (MB)	Peak Private Bytes (MB)	Avg. Working Set (MB)	Peak Working Set (MB)
Small Policy	Quarantine	AgentAPI	11.72	17.45	13.07	39.02
		AgntAsst	57.91	61.32	62.73	147.57
		AgntTray	7.01	7.71	4.12	10.18
	Dissolvable	AgntAsst	52.91	67.34	51.42	149.98
		DAgent	5.10	11.09	19.72	43.73
Medium Policy	Quarantine	AgentAPI	12.82	18.95	14.25	42.19
		AgntAsst	65.43	67.17	65.45	159.17
		AgntTray	7.79	8.41	4.01	12.08
	Dissolvable	AgntAsst	55.10	68.11	52.29	152.71
		DAgent	5.15	11.94	21.58	46.42
Large Policy	Quarantine	AgentAPI	14.16	22.15	17.64	49.48
		AgntAsst	68.75	70.22	67.32	168.59
		AgntTray	9.39	9.43	4.22	15.69
	Dissolvable	AgntAsst	58.60	71.25	55.71	161.94
		DAgent	5.96	13.34	24.08	49.76

Agent Required User Permissions

The Compliance Agent operates under any user mode. The Agent does not require local administrator privileges to execute and operates normally in restricted user mode.

Installing the Agent requires local administrative privileges, as do most MSI-based install programs. If the user cannot log on as a local administrator, the MSI can be executed with administrative rights using the “runas...” command. Additionally, since the Agent MSI is built using standard Windows Installer technology, it can be pushed to endpoints using common software distribution products.