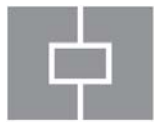


# SOPHOS



sophos **nac**

ADVANCED

Agent Deployment Guide



Copyright © 2010 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 December 2010

## Table of Contents

Agent Deployment Methods .....	4
Agent Install Parameters .....	4
Group Policy Logon Script.....	4
PsExec.....	6
Troubleshooting.....	6

## Agent Deployment Methods

This document provides information on how to deploy the Sophos Compliance Agent using either Group Policy Logon scripts or the Microsoft Sysinternals PsExec tool (<http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx>). If the installation is meant to be silent, then all parameters must be passed to the installer as additions to the MSI installation command. If these commands are not set properly, then the Agent will prompt the user for any information that was not set properly.

This document also provides information on how to use PsExec to push and install the Agent from the Compliance Application Server. With this method, you will need a list of IP addresses that you want to install to, as well as an Administrator's account that has full access on each of the computers. Using PsExec, the MSIExec attributes will be pushed to each computer in order to complete the installation process.

It is important to note that it is also possible to install the Agent using other tools such as SMS, CA Unicenter, and many more. However, this guide is meant to show how to install the Agent using two free, commonly-used tools.

**Important:** We recommend that only knowledgeable GPO users use this guide since doing something wrong can have undesired and potentially disastrous results.

## Agent Install Parameters

Agent parameters must be passed with the installation command to force the Agent to remain silent to the end user and install successfully. The Agent installation parameter descriptions can be found in further detail in the NAC Advanced Installation Guide, located at: [http://www.sophos.com/sophos/docs/eng/instguid/nacadv\\_32\\_seng.pdf](http://www.sophos.com/sophos/docs/eng/instguid/nacadv_32_seng.pdf)

Here is the list of possible parameters and the expected criteria for each:

AGENT\_SERVER – This parameter specifies the IP or DNS Name of the server.

AGENT\_INSTALLTYPE – Specifies the “Continuous” or “Quarantine” Agent, with “Quarantine” as the default.

AGENT\_SERVERMODE – Can be set to “HTTP” or “HTTPS”, with “HTTPS” as the default.

AGENT\_SETTINGS – This parameter should be used when utilizing the single sign-on feature, with the value “Register=usecomputerlogon”.

AGENT\_DHCPCLASS – Used to specify the User Class on the machine. This setting is usually used when the DHCP server doesn't support the DHCP Enforcer.

## Group Policy Logon Script

To install the Agent on each of the machines using Group Policy Object (GPO), you will need to create a script to set the command line parameters for the installer. Additionally, you must include logic to determine if the Agent is already installed. If you do not include the logic to determine installed status, the script will try to install the Agent each time the user logs in.

In this example, we are creating a VBScript that can run when the user logs in. The script will check for the existence of the Agent, and if the Agent is not present, it will run the installation. The GPO logon script should be located on the Domain Controller in a location reachable (shared SysVol location) by all of the client computers. If the computers cannot reach the script's location, then the script will not run, resulting in the computer not being able to install the Agent.

For computers to access the script, do the following:

1. Open Group Policy Management Console (GPMC).  
**Note:** GPMC is included on Windows Server 2008 and can be downloaded and installed for Windows Server 2003 from the following location: <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=0a6d4c24-8cbd-4b35-9272-dd3cbfc81887&displaylang=en>
2. Create a new Group Policy Object (GPO).
  - a. Right-click the Group Policy Objects as listed under the domain, and select **New**.
  - b. Type a name for the GPO, and leave the Source Starter GPO as none.
  - c. Click **OK** to create the new GPO.
3. Apply a Security Filter (group of users or computers) that the GPO should apply to.
  - a. Click the newly-created GPO, and select the **Scope** tab.
  - b. Click **Add** (under the Security Filtering), and select the Users, Computer, or Group that the GPO should apply to.
  - c. Click **OK** to close the dialog box.
4. Click the **Details** tab, and set the **GPO Status** to **Enabled**.
5. Right-click the GPO as listed under the domain, and select **Edit....**
6. In the Group Policy Management Editor, navigate to **Computer Configuration** or **User Configuration > Policies > Windows Settings**, and double-click **Scripts (Startup/Shutdown)** or **(Logon/Logoff)**. Options depend on whether Computer Configuration or User Configuration was selected.
7. Click **Startup** or **Logon** (in the right-hand navigation pane), and click **Add** to add the script to the Group Policy Management Editor. Click **Browse** to locate the script. By default, the GPO will open the directory to search for the script under a shared DC directory (i.e. \\DomainController\_Server\SysVol\DOMAIN\_NAME\Policies\{GUID}\Machine\Scripts\Startup).
8. When this location opens, drag the vbscript to this location, and then select it. The script should be present in the list of Startup\Logon scripts.
9. Once the script is in the correct location, close the Group Policy Management Editor, and drag the new GPO to the domain name (i.e. Group Policy Management -> Forest:Domain -> Domains -> Domain\_Name.com), and click **OK**. This will link the GPO to the domain.
10. The GPO is now enabled and linked to the domain. You can either wait for client computers to update their GPO settings to retrieve the script, or you can manually run "gpupdate /force" to force the client computers to download the GPO.

The following is a basic example for the VBScript installation. The installation command uses the "UseComputerLogon" parameter (described above) which can be used for the single sign-on feature. The MSI is pulled from the C\$ share on the Domain Controller (192.168.1.5) and creates an MSI log file in c:\ called nac32install.log:

```
Dim WshShell
Set WshShell = WScript.CreateObject("WScript.Shell")
Set objFS = CreateObject("Scripting.FileSystemObject")

'Confirm if NAC is installed
If (objFS.FileExists("c:\progra~1\Sophos\NAC\AgentAPI.exe")) Then
    WScript.quit

'If Not then run the installation
Else WshShell.run "cmd /c msiexec /i \\192.168.1.5\c$\SophosComplianceAgent.MSI
AGENT_INSTALLTYPE=quarantine AGENT_SETTINGS="UseComputerLogon"
AGENT_SERVER=efapp.endforce.com AGENT_SERVERMODE=HTTPS /qr /l*v c:\nac32install.log", 0,
True
End If

WScript.quit
```

## PsExec

The PsExec tool can be run from any server that it has been copied to. Make sure that the account that you specify in the installation command has Administrator rights for the computer that the Compliance Agent is installed on. The syntax for PsExec should be as follows:

```
PsExec.exe \\computer -u domain\user -p password Command_to_run_on_remote_computer
```

For additional parameters that can be used with this tool, consult Microsoft's guide located at:

<http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx>

Example Command:

```
PsExec.exe \\lab2-client -u lab\administrator -p password msieexec.exe /i "\\quadcore\software\SophosComplianceAgent.msi"  
AGENT_SERVER=172.16.205.164 AGENT_INSTALLTYPE=continuous AGENT_SERVERMODE=http  
AGENT_SETTINGS="Register=usecomputerlogon" /*v c:\installlog.txt
```

## Troubleshooting

### Group Policy Logon Script

In order to troubleshoot an issue with the Group Policy script, you will most likely need to review the Event Logs and the GPO settings that the machine has pulled down from the Domain Controller.

To review the Application Event logs, open the Event Viewer and look for events that come from "Userenv" or "Winlogon". Most likely, the errors/warnings coming from Userenv will be due to permissions errors. If there are errors present around permissions, ensure that the computer has access to the Group Policy information that is located on the Domain Controller's share. To see what GPOs were applied and which GPOs were filtered, run the "gpresult" command from the command line. If your new GPO was filtered, then it should give a reason to why the GPO was not applied, such as "Denied (Security)", which implies that the GPO did not have the correct security settings in place to be applied.

Microsoft provides further information on how to troubleshoot Group Policy issues at:

[http://technet.microsoft.com/en-us/library/cc775423\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc775423(WS.10).aspx)

[http://technet.microsoft.com/en-us/library/cc749336\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc749336(WS.10).aspx)

### PsExec Tool

The PsExec tool will capture the output from the remote computer when the command is run. If you receive errors around this process, mostly likely one of the following conditions is true:

- The command is trying to run the installation from a remote location, but a user/pass was not specified (-u / -p) in the command. This setting is necessary for network access on the remote computer.
- The syntax of the PsExec command is incorrect
- The user specified to run the process on the remote machine does not have permissions to execute it.

If any of the above conditions are true, then the installation will fail. For more information, consult the PsExec guide found at <http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx>, or perform an Internet search with your error.