

# SOPHOS

## Sophos NAC Advanced Application Management Solutions Guide

Product version: 3.2

Document date: May 2009



# Contents

|   |   |   |
|---|---|---|
| 1 | Integrating with Application Management Solutions.....                            | 3 |
| 2 | Configuring the Creation of the Assessment Results XML File.....                  | 4 |
| 3 | Configuring the Agent to Set the Location of the Assessment Results XML File..... | 5 |
| 4 | Configuring the Application Management Solution.....                              | 6 |
| 5 | Assessment Results XML File Format.....   | 7 |
| 6 | Copyright.....  | 9 |

# 1 Integrating with Application Management Solutions

Sophos NAC Advanced can be configured to provide raw assessment details for integration with application management solutions. During the policy assessment and enforcement processes, the software creates an XML file that contains information about the applications, service packs, OS patches, and operating systems that it has assessed on the endpoint. This file is placed in a location where it can be retrieved by the application management solution.

To configure Sophos NAC Advanced to integrate with application management solutions, you must complete two steps:

- Configure Sophos NAC Advanced to create the assessment results XML file.
- The path and name of the file containing these details is specified as an Agent setting.

## 2 Configuring the Creation of the Assessment Results XML File

To configure the creation of the assessment results XML file:

1. Locate the Policy Interface Web.config file on the Sophos Compliance Application Server. If you installed the software in the default location, the file can be found in the following location:  
c:\inetpub\wwwroot\PolicyInterface\Web.config.
2. Open the Web.config file in Notepad.
3. Locate the ExtraAgentProcessing section and the assessmentFile setting.
4. Change the **off** value to **on**.
5. Save and close the file.

**Note:** To stop the creation of the assessment results XML file, change the value in step 4 to off.

### 3 Configuring the Agent to Set the Location of the Assessment Results XML File

To specify the assessment results XML file location, you must create or update an Agent configuration template with the appropriate Agent setting, apply the Agent configuration template to a policy, and distribute the Agent file to endpoints. Once the Agent file is installed on the endpoint and the Agent assesses and enforces the policy, the Agent creates and saves the assessment results XML file in the location specified.

To configure the location of the assessment results XML file:

1. Log on to the Sophos Compliance Manager and click **Manage > Agent Configuration Templates > Create Agent Configuration Template** .

**Note:** You can also update an existing Agent configuration template. Click **Manage > Agent Configuration Templates** , and then click the name of the template you want to update.

2. Create an Agent configuration template that contains the appropriate Agent configuration settings.
3. In the Agent Customization section, click **Select**.
4. Select the **Assessment Results Path** check box, and click **OK**.
5. In the **Value** field, type the path and file name where you want the assessment results XML file to be saved on the endpoint, and click **Save** to create the Agent configuration template.

**Important:** The setting value must contain a valid path and file name. The path can contain supported replacement string variables (e.g., %EF\_ProgramFiles%).

6. Click **Manage > Policies > Create Policy** and create a policy with the Agent configuration template you just created.
7. Distribute the Agent to the appropriate endpoints.

Once the Agent file is installed on the endpoint and the Agent assesses and enforces the policy, the Agent creates and saves the assessment results XML file in the location specified. For more information on creating an Agent configuration template and policy, see the Compliance Manager help files.

## **4 Configuring the Application Management Solution**

You must also configure the application management solution to retrieve the assessment results XML file from the endpoint and configure what you want the application management solution to do with the assessment results XML file.

## 5 Assessment Results XML File Format

The following information is contained in the assessment results XML file:

- Version of the XML format
- Date and time of the last assessment (in endpoint local time)
- Last compliance state of the endpoint (compliant, partial, or nonCompliant)
- For each application assessed:
  - Application type (Agent App, AntiSpyware, AVApp, IDS App, OS, Patch, PFW App, any custom application types)
  - Application name
  - A flag indicating whether the application is installed
- For each capability assessed:
  - Capability type (isCurrent, isCurrentScanDate, lastScanDate, isRunning, isEnabled, version, servicePack, signatureDate, value, isRunningService)
  - Capability name
  - Result from the capability test

The following is a sample assessment results XML file:

```
<EF:CurrentAssessment xmlns:EF="ENDFORCE" version="3.0"
lastAssessment="8/26/2006
10:14:22 AM" lastComplianceState="nonCompliant">
  <EF:Application type="AVApp" name="Network Associates McAfee
Active VirusScan Suite"
installed="true">
  <EF:Capability type="version" name="Version" result="9.1" />
  <EF:Capability type="signatureDate" name="Signature Date"
result="08/22/2006" />
</EF:Application>
  <EF:Application type="PFW App" name="Network Associates McAfee
Desktop Firewall"
installed="true">
  <EF:Capability type="version" name="Version" result="8.0" />
</EF:Application>
  <EF:Application type="AntiSypware" name="McAfee Anti-Spyware
Corporate Edition"
installed="false" />
  <EF:Application type="OS" name="Windows XP" installed="true">
  <EF:Capability type="servicePack" name="Windows XP Service
Pack 2" result="true" />
</EF:Application>
```

```
<EF:Application type="Patch" name="Q886906" installed="true"
/>
<EF:Application type="Patch" name="Q903235" installed="false"
/>
</EF:CurrentAssessment>
```

## **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.