

AVGScan Component Documentation

Dokument Typ:

Version: 1.0

Datum: 27.01.2015

Autor: MWeber

Disclaimer: Copyright by x-dream-media GmbH. All Rights Reserved.
The information in this document may not be changed or
published without agreement of x-dream-media GmbH.

Table of contents

<u>1</u>	<u>Introduction</u>	<u>3</u>
<u>2</u>	<u>Functional Description</u>	<u>3</u>
2.1	File Inclusion and Exclusion	3
2.2	Pattern Matching	3
2.3	Inclusion/Exclusion by file size	3
<u>3</u>	<u>Error Handling</u>	<u>3</u>
<u>4</u>	<u>External Communication</u>	<u>4</u>
<u>5</u>	<u>External Setup</u>	<u>4</u>
<u>6</u>	<u>Agent Platforms</u>	<u>4</u>
<u>7</u>	<u>Inputs</u>	<u>4</u>
<u>8</u>	<u>Outputs</u>	<u>5</u>
<u>9</u>	<u>Logging</u>	<u>5</u>

Version

Datum	Version	Kapitel	Name	Änderung
27.01.15	1.0		mweber	Finalisierung Version 1.0

1 Introduction

The *AVGScan* component is an integration of the AVG virus scan software into the Signiant Workflow Engine. It takes a list of files and scans each file, using the AVG engine.

It is possible to include specific files only in the scan by changing the appropriate filter settings.

A range of AVG scan option is available as well.

This component is typically located in the *Antivirus* category of the workflow canvas toolbox.

2 Functional Description

The *AVGScan* component takes a list of files and makes use of the AVG antivirus engine to scan each file. Various filter can be applied to exclude certain files or include only specific files.

2.1 File Inclusion and Exclusion

Filters can be applied that will include and/or exclude files. Multiple filters must be separated with a comma and are applied with an *or* function.

If all files are to be scanned, the input field must not be empty but instead contain the *** character.

2.2 Pattern Matching

Special characters allow the use of pattern matching on the inclusion and exclusion filters. These characters are:

*	Matches zero or more characters. E.g.: <i>a*</i> matches <i>a, aa, aaaa</i>
?	Matches exactly one character. E.g.: <i>a?</i> matches <i>aa</i> , but not <i>a</i> or <i>aaa</i>
[...]	Matches character sets/ranges. E.g.: <i>example.[ch]</i> matches <i>example.c</i> and <i>example.h</i> , <i>example.[a-c]</i> matches <i>example.a, example.b</i> and <i>example.c</i> .

Limitations:

Leading *.* must be explicitly matched:

**.foo* does not match *.bar.foo*. For this you must specify the leading *.* like this: *.*.foo*.

2.3 Inclusion/Exclusion by file size

It is possible to exclude files from the scan that exceed a certain file size. The respective input field takes an integer, which the component handles as the maximum size in megabytes a file can have in order to be scanned. E.g.: *4000* excludes all the files from the scan that exceed 4GB in size.

3 Error Handling

Any errors encountered during execution of this component will result in the component exiting in failure. The Return Code output will be set to a non-zero value. Details about the error are written to the job log.

4 External Communication

The component makes use of the commandline tool of the AVG antivirus engine. In order for the component to be able to do so, the agent on which the software is installed and on which the component is set to run should be identical.

5 External Setup

AVG software needs to be installed on the agent running this component. The options for the scan itself are set by the component and do not require configuration of the AVG software (e.g. quarantine directory is defined in the component. The standard quarantine directory defined in the software is ignored).

6 Agent Platforms

All Signiant supported agent platforms may be used for this component, as long as the agent platform contains the installation of the AVG software including command line support.

7 Inputs

Name	Required	Default Value	Description
AVG Executable	yes		The path to the AVG command-line executable.
Filelist	yes		The list of files to be scanned. Can be either SigListXML or Legacy format (comma-separated list).
Patterns To Include	yes	*	A comma-separated list of strings/patterns. Only files matching these patterns are included in the scan.
Patterns To Exclude	no		A comma-separated list of strings/patterns. Files matching these patterns are excluded from the scan
Ignore Files Bigger Than	no	0	Takes an even number. If provided, all files bigger than the provide value (in megabytes) will be excluded from the scan.
Move Infected To Quarantine	yes	no	If <i>yes</i> is selected, files that failed the scan will be moved to the quarantine directory.
Quarantine Directory	no		Directory in which files, that failed the scan, are moved if <i>Move Infected To Quarantine</i> option is activated.
Priority	Yes	Auto	Available Options: Low, Auto, High – for more details consult the AVG documentation.
Heuristic Analysis	Yes	No	Activates AVG's <i>Heuristic Scan</i> options. For more details consult the AVG documentation.
Thorough Scan	Yes	No	Activates AVG's <i>Thorough Scan</i> option. For more details consult the AVG documentation
Archive Scanning	Yes	Yes	Activates AVG's <i>Archive Scanning</i> option. For more details consult the AVG documentation.
Potentially Unwanted Programs	Yes	Yes	Activates AVG's <i>Potentially Unwanted Programs</i> option. For more details consult the AVG documentation.

8 Outputs

Name	Description
Return Code	Set to zero if the component completes successfully. Set to non-zero if any errors occurred.
Return Message	A short message indicating the overall result of the component.
Passed Filelist	The list of files that passed the antivirus scan or were excluded from the scan due to filter settings. SigListXML encoded.
Failed Filelist	The list of files that failed the antivirus scan. If moved to a quarantine folder, includes the path to where the files were moved. SigList XML encoded.
Passed File Count	The number of files that passed the antivirus scan.
Failed File Count	The number of files that failed the antivirus scan.

9 Logging

All errors, debugging information and information about each scanned file is written to the job log.