

## Creating Custom AV Checks

This guide will help you create a custom Antivirus check. When a Cisco-created rule for an AV is not yet ready, you can create a custom check and rule to use to identify that AV.

First, you will need to identify a file or registry key that is modified every time the update process is run. Based on that, you can then do a custom check on the file date. For instance, for AVG Free version 8, the file `SYSTEM_PROGRAMS\AVG\AVG8\updatecomps.cfg` is the example we'll be using for this guide.

1. Navigate to Clean Access > Clean Access Agent > Rules > New Check
2. As we're checking a file, set the check category to "File Check".
3. Set the check type to "File Check".
4. Set the file path to the file we found earlier.
5. Set the operator to "Later than" and the file date to "CAM Date" – (however old you want to allow the definition files to be). For instance, if you want to allow the definition files to be 3 days old, put in "3".
6. Set the File Date Type to "Modification date".
7. Select the OSes you want this custom check to apply to.
8. Check "Automatically create rule based on this check".
9. Click on Add Check. This will now create a check and an associated rule for this check. Here's a screenshot of what this should look like, along with an overview of the configuration.

Certified Devices	General Setup	Network Scanner	CI
<a href="#">Distribution</a> · <a href="#">Installation</a> · <a href="#">Rules</a> · <a href="#">Requirements</a> · <a href="#">Role-Requirements</a> · <a href="#">Reports</a>			
<a href="#">Check List</a>   <a href="#">New Check</a>   <a href="#">Rule List</a>   <a href="#">New Rule</a>   <a href="#">New AV Rule</a>   <a href="#">New AS Rule</a>   <a href="#">AV/AS Support Info</a>			
Check Category	File Check		
Check Name	AVGDefinitions-customcheck		
File Path	SYSTEM_PROGRAMS	\AVG\AVG8\updatecomps.cfg	
Operator	later than		
File Date	<input type="radio"/> (mm/dd/yyyy hh:MM:ss) <input checked="" type="radio"/> CAM date (midnight) - 3 days		
File Date Type	<input type="radio"/> Creation date <input checked="" type="radio"/> Modification date		
Check Description	Custom check for AVG		
Operating System	<input type="checkbox"/> Windows All <input type="checkbox"/> Windows 2000 <input checked="" type="checkbox"/> Windows XP (All) <input type="checkbox"/> XP Pro/Home <input checked="" type="checkbox"/> Windows Vista (All) <input type="checkbox"/> XP Tablet PC <input type="checkbox"/> Vista Home Basic <input type="checkbox"/> XP Media Center <input type="checkbox"/> Vista Home Premium <input type="checkbox"/> Vista Business <input type="checkbox"/> Vista Ultimate <input type="checkbox"/> Vista Enterprise <input checked="" type="checkbox"/> Windows 7 (All) <input type="checkbox"/> 7 Starter <input type="checkbox"/> 7 Home Basic <input type="checkbox"/> 7 Home Premium <input type="checkbox"/> 7 Professional <input type="checkbox"/> 7 Enterprise <input type="checkbox"/> 7 Ultimate		
<input checked="" type="checkbox"/> Automatically create rule based on this check <input type="button" value="Add Check"/>			

Check Category: File Check

Check Type: File Date

File Path: SYSTEM\_PROGRAMS \AVG\AVG8\updatecomps.cfg

Operator: later than

File Date: CAM Date - (however old you will allow the definition files to be, i.e. 3 for 3 days)

File Data Type: Modification Date

Operating System: your choice

Check "Automatically create rule based on this check".

10. You can click on Rule List to verify that the rule was automatically created.

11. Next, we need to tie the new rule to the already existing AV update requirement. Click on Requirements > Requirements-Rules, and select your AV Definition requirement. You can determine which requirement is your AV Definition requirement from the Requirements > Requirement List page, and finding the one whose Type is "AV Definition".

12. Change the Requirement met if: field to “Any selected rule succeeds”, and make sure the OS is set to one of the operating systems you created the check for.
13. Scroll down until you find the new rule you just created, and click on the checkbox next to it. The way the requirement will now work is that it will check both the previous AV rule and your new custom rule. If either succeeds, then the user will pass the requirement.

<input type="checkbox"/>	NAC-Registry-Check-rule	Win ( All )
<input checked="" type="checkbox"/>	AVGDefinitions-customcheck-rule	Win ( 7 (All), Vista (All), XP (All) )
<input type="checkbox"/>	any valid av	Win ( 7 (All), Vista (All), XP (All), 2000 )

14. You will most likely need to check the box next to the rule for each OS (ie Windows 7 (all), Windows Vista (all), Windows XP (all), Windows 2000). Select another OS from the dropdown box at the top of the page, and then make sure to check the box next to the new rule.