

NAC Appliance (Clean Access): Configure And Troubleshoot the Antivirus Definition Updates

Document ID: 97868

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure AV Definition Update Requirements

- AV Rules
- Verify AV Support Information
- Create AV Rule
- Create AV Definition Update Requirement
- Map Requirement to Rules
- Apply Requirements to Role
- Validate Requirements
- Cisco Rules
- Cisco Checks
- Cisco Pre-Configured Rules (pr_)

Troubleshoot

- Cisco Clean Access Does Not Update AV Definition for Clients
- CCA Not Detect AV

Related Information

Introduction

This document describes how to configure and troubleshoot the Antivirus (AV) Definition Update requirements in the Cisco Network Admission Control (NAC) Appliance, formerly known as Cisco Clean Access.

Prerequisites

Requirements

This document assumes that Cisco Clean Access, which includes both Clean Access Manager (CAM) and Clean Access Server (CAS), is installed and works properly.

Components Used

The information in this document is based on Cisco Clean Access 3.4 and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

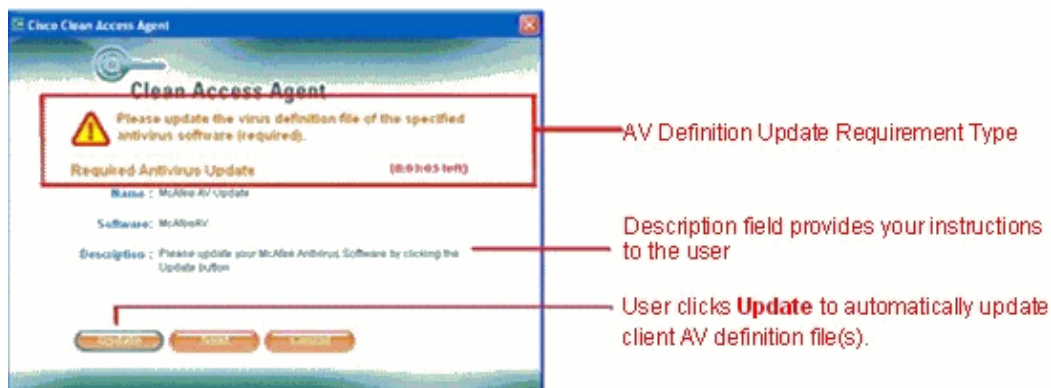
Configure AV Definition Update Requirements

The **AV Definition Update** requirement type can be used in order to update the definition files on a client for supported antivirus products. If the client fails to meet the AV requirement, the Clean Access Agent communicates directly with the installed antivirus software on the client and automatically updates the definition files when the user clicks the **Update** button on the Agent dialog.

AV Rules incorporate extensive logic for 24 antivirus vendors and are associated with AV Definition Update requirements. For AV Definition Update requirements, the configuration is similar to that of custom requirements, except there is no need to configure checks. You associate AV Definition Update requirements with one or more AV Rules, user roles and operating systems and also configure the Clean Access Agent dialog instructions you want the user to see if the AV requirement fails.

Note: Where possible, it is recommended to use AV Rules mapped to AV Definition Update requirements in order to check antivirus software on clients. In the case of a non-supported AV product, or if an AV product or version is not available through AV Rules, you always have the option to use Cisco provided pc_checks and pr_rules for the antivirus vendor or to create their own custom checks, rules, and requirements through **Device Management > Clean Access > Clean Access Agent**. Use New Check, New Rule, and New File/Link/Local Check Requirement.

This figure shows the Clean Access Agent dialog that appears when a client fails to meet an AV Definition Update requirement.



AV Rules

AV Rules are preconfigured rule types mapped to the matrix of vendors and products sourced in the Supported AV Product List. There is no need to configure checks with this type of rule.

There are two basic types of AV Rules:

- **Installation AV Rules** This rule checks whether the selected antivirus software is installed for the client OS.
- **Virus Definition AV Rules** This rule checks whether the virus definition files are up-to-date on the client. Virus Definition AV Rules can be mapped into AV Definition Update requirements so that a user that fails the requirement can click the Update button in the Agent in order to automatically execute the update.

AV Rules are typically associated with AV Definition Update requirements. These steps are required in order to create AV Definition Update requirements:

1. Verify AV Support Information
2. Create AV Rule
3. Create AV Definition Update Requirement
4. Map Requirement to Rules
5. Apply Requirements to Role
6. Validate Requirements

Verify AV Support Information

The Cisco NAC Appliance allows multiple versions of the Clean Access Agent to be used on the network. New updates to the Agent add support for the latest antivirus products as they are released. The system picks the best method, either Def Date or Def Version in order to execute AV definition checks based on the AV products available and the version of the Agent. The AV Support Info page provides details on Agent compatibility with the latest Supported AV Product List downloaded to the CAM. This page lists the latest version and date of definition files for each AV product as well the baseline version of the Agent needed for product support. You can compare the AV information of the client against the AV Support Info page in order to verify that the definition file a client has is the latest. If you run multiple versions of the Agent on your network, this page can help troubleshoot which version must be run in order to support a particular product.

Complete these steps in order to view Agent support details:

1. Choose **Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info**.
2. Choose **Antivirus** from the Category drop-down menu.

Minimum Agent Version Required to Support AV Products			
Product Name/Version	Installation	Virus Definition	
		Def Date	Def Version
AOL Safety and Security Center Virus Protection 1.x	3.6.1.0	3.6.1.0	3.6.1.0

Latest Virus Definition Version/Date for Selected Vendor			
Product Name	Version	Type	Value
ALL	ALL	Version	4700
ALL	ALL	Date	02/17/2006

3. Choose an **Antivirus Vendor** from the drop-down menu.
4. Choose **Windows Vista/XP/2K** or **Windows 9x/ME** from the **Operating System** drop-down menu in order to view the support information for those client systems. This populates the tables as shown:
 - a. **Minimum Agent Version Required to Support AV Products** shows the minimum Agent version required in order to support each AV product. For example, a 4.0.0.0 Agent can log into a role that requires AOL Safety and Security Center Virus Protection 1.x, but for a 3.6.0.0 or earlier Agent, this check fails. Note that if a version of the Agent supports both Def Date and Def Version checks, the Def Version check is used.
 - b. **Latest Virus Definition Version/Date for Selected Vendor** displays the latest version and date information for the AV product. The AV software for an up-to-date client must display

the same values.

Note: The Agent sends its version information to the CAM, and the CAM always attempts to use the virus definition version for AV checks first. If the version is not available, the CAM uses the virus definition date instead.

Tip: You can also view the latest definition file version when you choose an AV vendor from the **New AV Rule** form.

Create AV Rule

Complete these steps in order to create an AV Rule:

1. Make sure you have the latest version of the Supported AV/AS Product List.
2. Choose **Device Management > Clean Access > Clean Access Agent > Rules > New AV Rule**.

Checks for Selected Operating Systems			
Product Name	Version	Installation	Virus Definition
ANY	ANY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Norton AntiVirus	10.x	<input type="checkbox"/>	<input type="checkbox"/>
Norton AntiVirus 2002	8.00.x	<input type="checkbox"/>	<input type="checkbox"/>
Norton AntiVirus 2002	8.x	<input type="checkbox"/>	(Not Supported)
Norton AntiVirus 2002 Professional	8.x	<input type="checkbox"/>	<input type="checkbox"/>
Norton AntiVirus 2002 Professional Edition	8.x	<input type="checkbox"/>	<input type="checkbox"/>
Norton AntiVirus 2003	9.x	<input type="checkbox"/>	<input type="checkbox"/>
Norton AntiVirus 2003 Professional	9.x	<input type="checkbox"/>	<input type="checkbox"/>
Norton AntiVirus 2003 Professional Edition	9.x	<input type="checkbox"/>	<input type="checkbox"/>

3. Type a **Rule Name**. You can use digits and underscores, but no spaces in the name.
4. Choose an **Antivirus Vendor** from the drop-down menu. This populates the **Checks for Selected Operating Systems** table at the bottom of the page with the supported products and product versions from this vendor for the selected **Operating System**.
5. From the **Type** drop-down menu, choose either **Installation** or **Virus Definition**. This enables the check boxes for the corresponding Installation or Virus Definition columns in the table.
6. Choose an **Operating System** from the drop-down menu, either Windows Vista/XP/2K or Windows ME/98. This displays the product versions supported for this client OS in the table.
7. Type an optional **Rule Description**.
8. In the **Checks for Selected Operating Systems** table, choose the product versions you want to check for on the client. In order to do this, check one or more check boxes in the corresponding **Installation** or **Virus Definition** columns. **ANY** means you want to check for any product and any version from this AV vendor. **Installation** checks whether the product is installed, and **Virus Definition** checks whether the virus definition files are up-to-date on the client for the specified product.
9. Click **Add Rule**. The new AV rule is added at the bottom of the **Rule List** with the name you provided.

Create AV Definition Update Requirement

These steps show how to create a new AV Definition Update requirement in order to check the client system for the specified AV products and versions with an associated AV Rule. If the antivirus definition files of the client are not up-to-date, the user can simply click the **Update** button on the Clean Access Agent, and the Agent causes the resident AV software to launch its own update mechanism. Note that the actual mechanism differs for different AV products, for example, live updates versus command line parameter.

1. On the **Clean Access Agent** tab, click the **Requirements** submenu link, and then **New Requirement**.

The screenshot shows the 'Clean Access Agent' configuration window. The 'Requirements' submenu is active, and the 'New Requirement' option is selected. The 'Requirement Type' is set to 'AV Definition Update'. The 'Do not enforce requirement' checkbox is checked. The 'Priority' is set to 1. The 'Antivirus Vendor Name' is set to 'ANY'. The 'Requirement Name' is 'Any_AV_UpToDate_WinXP_Vista'. The 'Description' is 'Your Anti-Virus definition files are not up-to-date. Please'. The 'Operating System' section has checkboxes for 'Windows All', 'Windows 2000', 'Windows ME', 'Windows 98', 'Windows XP (All)', 'XP Pro/Home', 'XP Tablet PC', 'XP Media Center', 'Windows Vista (All)', 'Vista Home Basic', 'Vista Home Premium', 'Vista Business', 'Vista Ultimate', and 'Vista Enterprise'. The 'Add Requirement' button is visible. Below the form, there is a note and a table titled 'Product versions supported for Update via Clean Access Agent'.

OS	Product versions supported for Update via Clean Access Agent
Windows XP/2000	All products supported on Windows XP and Windows 2000
Windows ME/98	All products supported on Windows ME and Windows 98

2. For **Requirement Type** choose **AV Definition Update**.
3. The **Do not enforce requirement** option is checked by default, which designates the AV Definition Update requirement as **optional**.

Note: Because the Windows Update process runs in the background, **Do not enforce requirement** is set by default in order to optimize the user experience. It is recommended to leave this requirement as optional if you choose the Automatically download and install option. A WSUS forced update can take a while, and is launched and run in the background.

4. Choose the **Priority** of execution for this requirement on the client. A high priority, such as 1, means this requirement is checked on the system ahead of all other requirements and appears in the Agent dialogs in that order. Note that if a mandatory requirement fails, the Agent does not continue past that point until that requirement succeeds.
5. Choose an **Antivirus Vendor Name** from the drop-down menu. The **Products** table lists all the virus definition product versions supported for each client OS.
6. For the **Requirement Name**, type a unique name to identify this AV definition file requirement in the Agent. The name is visible to users on the Clean Access Agent dialogs.
7. In the **Description field**, type a description of the requirement and instructions to guide users who fail to meet the requirement. For an AV Definition Update requirement, you must include instructions for users to click the **Update** button in order to update their systems. Keep this information in mind:

- ◆ **AV Definition Update** displays the **Update** button on the Agent.

- ◆ **AS Definition Update** displays the **Update** button on the Agent.
 - ◆ **Windows Update** displays the **Update button** on the Agent.
8. Check one or more of these check boxes in order to set the **Operating Systems** for the requirement:
- ◆ **Windows All**
 - ◆ **Windows 2000**
 - ◆ **Windows ME**
 - ◆ **Windows 98**
 - ◆ **Windows XP (All) or one or more of the specific Windows XP operating systems**
 - ◆ **Windows Vista (All) or one or more of the specific Windows Vista operating systems**
9. Click **Add Requirement** in order to add the requirement to the Requirement List.

Map Requirement to Rules

Once the requirement is created and the remediation links and instructions are specified, map the requirement to a rule or set of rules. A requirement-to-rule mapping associates the ruleset that checks whether the client system meets the requirement to the user requirement action (Agent button, instructions, links) needed in order for the client system to comply.

1. On the **Clean Access Agent** tab, click the **Requirements** submenu, and then open the **Requirement-Rules** form.

Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent

Distribution | Rules | Requirements | Role-Requirements | Reports | Updates

Requirement List | New Requirement | Requirement-Rules

Requirement Name: Any_AV_UpToDate_WinAll | Operating System: Windows XP

Requirement met if:

- All selected rules succeed
- Any selected rule succeeds
- No selected rule succeeds

*Note: The service of providing regularly updated Spyware definition data/version is not available on the Cisco terminal yet. For AS Spyware Definition rules, this system has enforced the feature of allowing the definition file to be X days older than the current system date. Once the service is available, this note will be automatically removed.

For AV Virus Definition rules, allow definition file to be 0 days older than

- the latest file date
- current system date

For AS Spyware Definition rules, allow definition file to be 0 days older than

- the latest file date
- current system date

Rules for Selected Operating System | Update

Select	Name	OS
<input type="checkbox"/>	pr_AutoUpdateCheck_Rule	Win { XP,2000 }
<input type="checkbox"/>	pr_XP_Hotfixes	Win { XP }
<input type="checkbox"/>	pr_Symantec_Client_Firewall_Enable	Win { XP }

2. From the **Requirement Name** menu, choose the requirement to map.
3. Verify the operating system for the requirement in the **Operating System** menu. The **Rules for Selected Operating System** list is populated with all rules available for the chosen OS.
4. For AV Virus Definition Rules (yellow background), you can optionally configure the CAM to allow definition files on the client to be a number of days older than what the CAM has available from **Updates**. See **Rules > AV-AS Support Info** for the latest product file dates. This allows you to configure leeway into a requirement so that if no new virus definition files are released from a product vendor, your clients can still pass the requirement. In order to do this, complete these steps:

- a. Check the **AV Virus Definition rules, allow definition file to be x days older than** check box.
- b. Type a number in the text box. The default is **0**, which indicates the definition date cannot be older than the file/system date.
- c. Select one of these options:

- ◇ **Latest file date** This allows the client definition file to be older than the latest virus definition date on the CAM by the number of days you specify.
- ◇ **Current system date** This allows the client definition file to be older than the CAM system date when the last **Update** was performed by the number of days you specify.

5. Scroll down the page and check the **Select** check box next to each rule you want to associate with the requirement. The rules are applied in their order of priority, as described in this table:

<input type="checkbox"/>	Any_AV_Installed_XP2K	Win (XP,2000)
<input checked="" type="checkbox"/>	Any_AV_Def_XP2K	Win (XP,2000)
<input type="checkbox"/>	Lavasoft_Any_Installaben	Win (XP,2000)
<input type="checkbox"/>	Lavasoft_Any_Definbon	Win (XP,2000)
<input type="checkbox"/>	Check-for-3600-or-above-Agent-rule	Win (All)
<input type="checkbox"/>	Spybot_Any_Install	Win (XP,2000)
<input type="checkbox"/>	Spybot_13_Install	Win (XP,2000)
<input type="checkbox"/>	Spybot_Any_Def	Win (XP,2000)

6. For **Requirements met if**, choose one of these options:

- ◆ **All selected rules succeed** if all the rules must be satisfied in order for the client to be considered in compliance with the requirement
- ◆ **Any selected rule succeeds** if at least one selected rule must be satisfied in order for the client to be considered in compliance with the requirement
- ◆ **No selected rule succeeds** if the selected rules must all fail in order for the client to be considered in compliance with the requirement

If clients are not in compliance with the requirement, they must install the software associated with the requirement or complete the required steps.

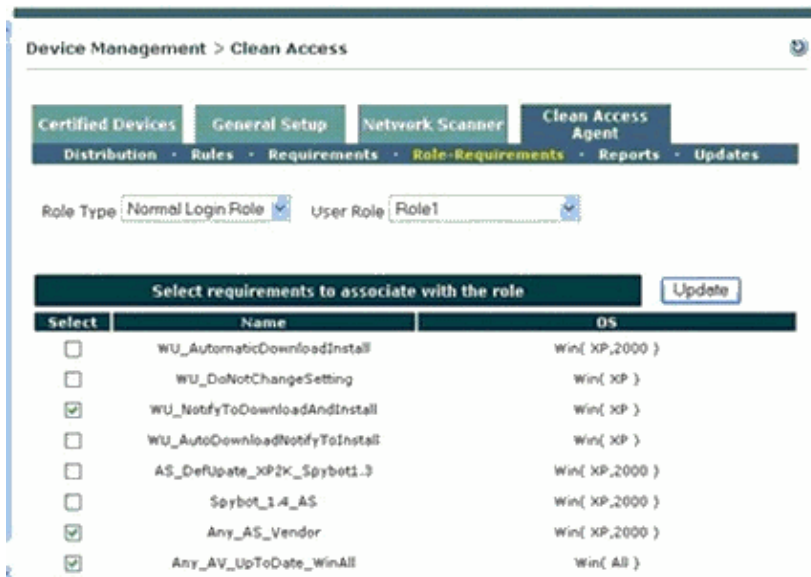
7. Click **Update**.

Apply Requirements to Role

Once requirements are created, configured with remediation steps, and associated with rules, they need to be mapped to user roles. This step applies your requirements to the user groups in the system.

Note: Make sure you already have normal login user roles created.

1. On the **Clean Access Agent** tab, click the **Role–Requirements** submenu link.



2. From the **Role Type** menu, choose the type of the role to configure. In most cases, this is **Normal Login Role**.
3. Choose the name of the role from the **User Role** menu.
4. Check the **Select** check box for each requirement you want to apply to users in the role.
5. Click **Update**.
6. Before you finish, make sure users in the role are required to use the Clean Access Agent.

Validate Requirements

The Clean Access Manager automatically validates requirements and rules as they are created. The **Validity** column under **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement List** displays requirement validity, as shown:

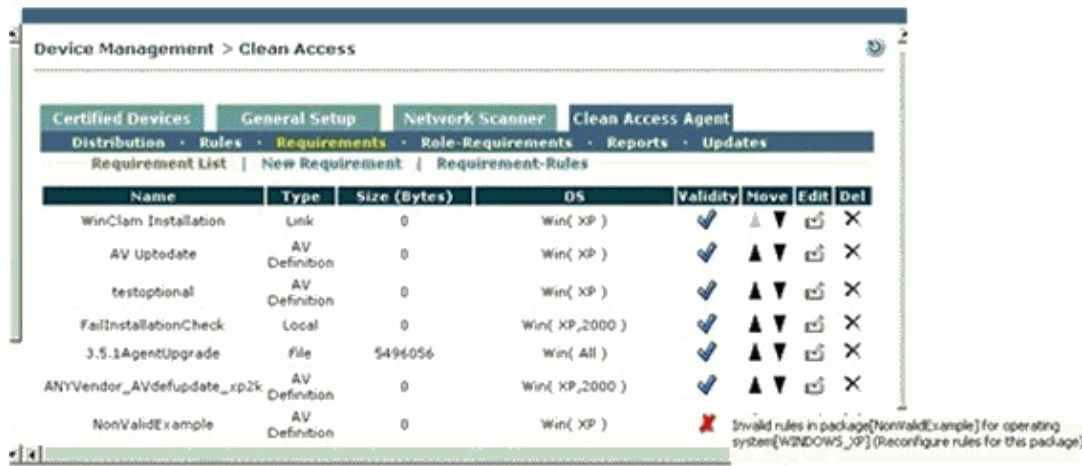
- The requirement is valid.
- The requirement is invalid. Highlight this icon with your mouse in order display the validity status message for this requirement. The status message states which rule and which check causes the requirement to be invalid, in this format:

```
Invalid rule [rulename] in package [requirementname] (Rule verification error:
Invalid check [checkname] in rule expression)
```

The requirement must be corrected and made valid before it can be used. Typically, requirements and rules become invalid when there is an operating system mismatch.

In order to correct an invalid requirement, complete these steps:

1. Choose **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement–Rules**.
2. Correct any invalid rules or checks.
3. Choose the invalid **Requirement Name** from the drop–down menu.
4. Choose the **Operating System**.
5. Make sure the **Requirement met if:** expression is correctly configured.
6. Make sure the rules selected for the requirement are valid, which means they have a blue check mark in the Validity column.



Status message for invalid requirement

Cisco Rules

A rule is a conditional statement made up of one or more checks. A rule combines checks with logical operators in order to form a Boolean statement that can test multiple features of the client system.

The Cisco NAC Appliance provides a set of pre-configured rules and checks through the Updates link. Pre-configured rules have a prefix of `pr` in their names, such as `pr_AutoUpdateCheck_Rule`. See Cisco Pre-Configured Rules ("pr_") for more information.

Cisco Checks

A check is a conditional statement that examines a feature of the client system, such as a file, registry key, service, or application. Pre-configured checks have a prefix of `pc` in their names, such as `pc_Hotfix828035`. This table lists the types of checks available and what they test.

Check Category	Check Type
Registry check	<ul style="list-style-type: none"> • whether or not a registry key exists • registry key value
File Check	<ul style="list-style-type: none"> • whether or not a file exists • date of modification or creation • file version
Service check	<ul style="list-style-type: none"> • whether or not a service runs
Application check	<ul style="list-style-type: none"> • whether or not an application runs

Cisco Pre-Configured Rules (pr_)

The Cisco NAC Appliance provides a set of pre-configured rules and checks that are downloaded to the CAM through the **Updates** page on the CAM web console, under **Device Management > Clean Access >**

Clean Access Agent > Updates.

Pre-configured rules have a prefix of `pr` in their names, for example `pr_XP_Hotfixes`, and can be copied for use as a template, but cannot be edited or removed. You can click the **Edit** button for any `pr_` rule in order to view the rule expression that defines it. The rule expression for a pre-configured rule is composed of pre-configured checks, such as `pc_Hotfix835732`, and boolean operators. The rule expression for pre-configured rules is updated through Cisco Updates. For example, when new Critical Windows OS hotfixes are released for Windows XP, the `pr_XP_Hotfixes` rule is updated with the related hotfix checks.

Pre-configured rules are listed under **Device Management > Clean Access > Clean Access Agent > Rules > Rule List**. Pre-configured checks have a prefix of `pc` in their names and are listed under **Device Management > Clean Access > Clean Access Agent > Rules > Check List**.

Note: Cisco pre-configured rules are intended to provide support for Critical Windows OS hotfixes only.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Cisco Clean Access Does Not Update AV Definition for Clients

Complete these steps in order to resolve this issue:

1. In the CAM, choose **Device Management > Clean Access > Requirements > Requirement-Rules**.
2. Deselect the pre-configured rules (`pr_`), if any.
3. Select the appropriate AV rules.

CCA Not Detect AV

If you suspect the CCA does not detect or recognize the certain AV checks, then you need to run the OESIS diagnostic tool in the client.

Complete these steps:

1. Enable logging.

Refer to [Enable Debug Logging on the Clean Access Agent](#) for the instructions on how to enable debug logging on the client.

2. Attempt to login.
3. Run the OESIS diagnose tool.
4. Disable logging.

Note: If you can grab an export of the registry key structure from the AV product, normally located at `HKLM\Software\<av_vendor>`, that is helpful too.

Related Information

- [Cisco NAC Appliance \(Clean Access\) Support Page](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

