

# НАС-устройство (Cisco Clean Access): Настройка и устранение неполадок обновлений определений антивируса

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройте требования обновления определения AV](#)

[Правила AV](#)

[Проверьте сведения о поддержке AV](#)

[Создайте правило AV](#)

[Создайте требование обновления определения AV](#)

[Требование карты к правилам](#)

[Примените требования к роли](#)

[Проверьте требования](#)

[Правила Cisco](#)

[Проверки Cisco](#)

[Cisco предварительно сконфигурированные правила \("PR "\)](#)

[Устранение неполадок](#)

[Cisco Clean Access не обновляет определение AV для клиентов](#)

[ССА, неспособный обнаружить AV](#)

[Дополнительные сведения](#)

## **Введение**

Этот документ описывает, как настроить и устранить неполадки Антивируса (AV) требования Обновления Определения в системе контроля доступа к сети Cisco NAC (NAC) Устройство, раньше известное как Cisco Clean Access.

## **Предварительные условия**

### **Требования**

Этот документ предполагает, что Cisco Clean Access, который включает и Clean Access Manager (CAM) и чистый сервер доступа (CAS), установлен и работает должным образом.

## Используемые компоненты

Сведения в этом документе основываются на Cisco Clean Access 3.4 и позже.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

## Условные обозначения

[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

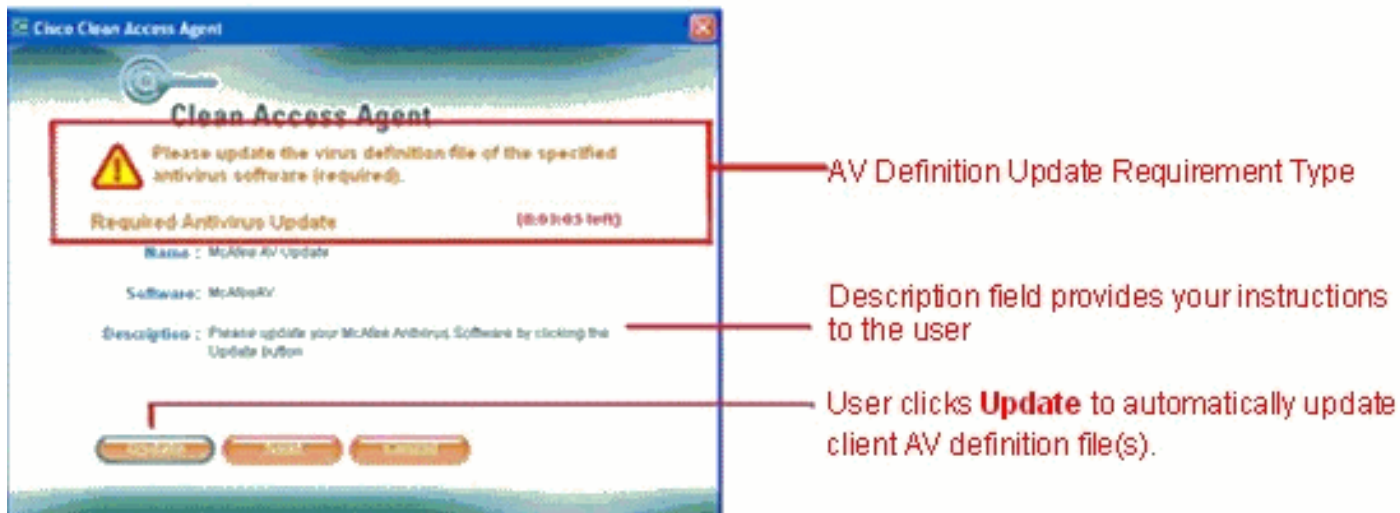
## Настройте требования обновления определения AV

Тип требования **Обновления Определения AV** может использоваться для обновления файлов определения на клиенте для поддерживаемых антивирусных продуктов. Если клиент не в состоянии удовлетворять требование AV, Чистый Агент Доступа связывается непосредственно с установленным антивирусным программным обеспечением на клиенте и автоматически обновляет файлы определения, когда пользователь нажимает кнопку **Update** на диалоговом окне Агента.

Правила AV включают обширную логику для 24 антивирусных поставщиков и привязаны к требованиям Обновления Определения AV. Для требований Обновления Определения AV конфигурация подобна тому из пользовательских требований, кроме нет никакой потребности настроить проверки. Вы привязываете требования Обновления Определения AV к одному или более Правилам AV, ролям пользователя и операционным системам и также настраиваете Чистые диалоговые инструкции Агента Доступа, которые вы хотите, чтобы пользователь видел, отказывает ли требование AV.

**Примечание:** Где возможно, рекомендуется использовать Правила AV, сопоставленные с требованиями Обновления Определения AV для проверки антивирусного программного обеспечения на клиентах. В случае неподдерживаемого продукта AV, или если продукт AV или версия не доступны через Правила AV, у вас всегда есть опция, чтобы использовать предоставленный [pc checks](#) Cisco и [pr rules](#) для антивирусного поставщика или создать их собственные проверки, правила и требования через **Управление устройствами> Чистый Доступ> Чистый Агент Доступа**. Используйте Новую Проверку, Новое Правило и Новое Требование Проверки Файла/Ссылки/Локального.

Эти данные показывают Чистое диалоговое окно Агента Доступа, которое появляется, когда клиент не в состоянии удовлетворять требование Обновления Определения AV.



## Правила AV

Правила AV предварительно сконфигурированы типы правила, сопоставленные с матрицей поставщиков и продуктов, полученных в Поддерживаемом Списке продуктов AV. Нет никакой потребности настроить, сверяется с этим типом правила.

Существует два базовых типа Правил AV:

- **Правила AV установки** — Это правило проверяет, установлено ли выбранное антивирусное программное обеспечение для клиентской операционной системы.
- **Правила AV Определения вируса** — Это правило проверяет, актуальны ли файлы определения вируса на клиенте. Правила AV Определения вируса могут быть сопоставлены в требования Обновления Определения AV так, чтобы пользователь, который отказывает требование, мог нажать кнопку Update в Агенте для автоматического выполнения обновления.

Правила AV, как правило, привязываются к требованиям Обновления Определения AV. Эти шаги требуются для создания требований Обновления Определения AV:

1. [Проверьте сведения о поддержке AV](#)
2. [Создайте правило AV](#)
3. [Создайте требование обновления определения AV](#)
4. [Требование карты к правилам](#)
5. [Примените требования к роли](#)
6. [Проверьте требования](#)

## Проверьте сведения о поддержке AV

Устройство Cisco NAC позволяет нескольким версиям Чистого Агента Доступа использоваться в сети. Новые обновления Агента добавляют поддержку последних антивирусных продуктов, поскольку они освобождены. Система выбирает лучший метод, или Версия Даты или Def Def для выполнения проверок определения AV на основе доступных продуктов AV и версия Агента. Страница AV Support Info предоставляет подробную информацию о совместимости Агента с последним Поддерживаемым Списком продуктов AV, загруженным к CAM. Эта страница перечисляет последнюю версию и дату файлов определения для каждого продукта AV также базовая версия Агента, необходимого для поддержки продуктов. Можно сравнить информацию о AV клиента против страницы AV

Support Info, чтобы проверить, что файл определения, который имеет клиент, является последним. При выполнении нескольких версий Агента в сети эта страница может помочь устранять неполадки, какая версия должна быть выполнена для поддержки конкретного продукта.

Выполните эти шаги, чтобы посмотреть детали Поддержки агента:

1. Выберите **Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info**.
2. Выберите **Antivirus** из раскрывающегося меню Категории.

The screenshot shows the 'AV/AS Support Info' page in the Clean Access Agent interface. The page is titled 'Device Management > Clean Access' and has several tabs: 'Certified Devices', 'General Setup', 'Network Scanner', and 'Clean Access Agent'. Under 'Clean Access Agent', there are sub-tabs: 'Distribution', 'Rules', 'Requirements', 'Role-Requirements', 'Reports', and 'Updates'. The 'Rules' tab is selected, and there are links for 'Check List', 'New Check', 'Rule List', 'New Rule', 'New AV Rule', 'New AS Rule', and 'AV/AS Support Info'.

The 'Category' dropdown is set to 'Antivirus'. The 'Antivirus Vendor' dropdown is set to 'America Online, Inc.'. The 'Operating System' dropdown is set to 'Windows Vista/XP/2K'.

Below the dropdowns, there are two tables:

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. Выберите **Antivirus Vendor** из раскрывающегося меню.
4. Выберите **Windows Vista/XP/2K** или **Windows 9x/ME** от раскрывающегося меню **Операционной системы** для просмотра сведений о поддержке для тех систем клиента. Это заполняет таблицы как показано: **Минимальная Версия агента, Требуемая для Поддержки продуктов AV** — показывает, что минимальная Версия агента потребовалась для поддержки каждого продукта AV. Например, 4.0.0.0 Агента могут войти в роль, которая требует Антивирусной защиты Центра Безопасности AOL 1.x, но для 3.6.0.0 или более раннего Агента, эта проверка сбой. Обратите внимание на то, что, если версия Поддержек агента и Проверки версии Даты и Def Def, используется Проверка версии Def. **Версия/Дата Свежего описания вирусов для Выбранного Поставщика** — отображает последнюю версию и информацию о дате для продукта AV. Программное обеспечение AV для актуального клиента должно отобразить те же значения.

**Примечание:** Агент передает его сведения о версии к САМ, и САМ всегда пытается использовать версию определения вируса для проверок AV сначала. Если версия не доступна, САМ использует дату определения вируса вместо этого.

**Совет:** Можно также посмотреть последнюю версию файла определения при выборе поставщика AV из **Новой формы Правила AV**.

## [Создайте правило AV](#)

Выполните эти шаги для создания Правила AV:

1. Удостоверьтесь, что у вас есть последняя версия Поддерживаемого Списка продуктов AV/AS.
2. Выберите **Device Management > Clean Access > Clean Access Agent > Rules > New AV Rule**.

The screenshot shows the 'New AV Rule' configuration page. The breadcrumb path is 'Device Management > Clean Access'. The page has several tabs: 'Certified Devices', 'General Setup', 'Network Scanner', and 'Clean Access Agent'. Under 'Clean Access Agent', there are sub-tabs: 'Distribution', 'Rules', 'Requirements', 'Role-Requirements', 'Reports', and 'Updates'. The 'Rules' sub-tab is active, and the 'New AV Rule' link is selected.

The form fields are as follows:

- Rule Name: Any\_Symantec\_VirusDef
- Antivirus Vendor: Symantec Corp.
- Type: Virus Definition
- Operating System: Windows Vista/XP/2K
- Rule Description: Check for any up-to-date Symantec AV

There is an 'Add Rule' button below the form.

Below the form is a table titled 'Checks for Selected Operating Systems'.

Product Name	Version	Installation	Virus Definition
ANY	ANY	<input checked="" 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. Введите **Имя правила**. Можно использовать цифры и подчеркивания, но никакие пробелы на название.
4. Выберите **Antivirus Vendor** из раскрывающегося меню. Это заполняет **Проверки для Выбранной** таблицы **Операционных систем** внизу страницы с поддерживаемыми продуктами и версиями продукта от этого поставщика для выбранной **Операционной системы**.
5. От раскрывающегося меню **Типа** выберите **Installation** или **Virus Definition**. Это включает флажки для соответствующих столбцов Installation или Virus Definition в таблице.
6. Выберите **Operating System** из раскрывающегося меню, или Windows Vista/XP/2K или Windows ME/98. Это отображает версии продукта, поддерживаемые для этой клиентской операционной системы в таблице.
7. Введите дополнительное **Описание Правила**.
8. В **Проверках для Выбранной** таблицы **Операционных систем** выберите версии продукта, для которых вы хотите проверить на клиенте. Чтобы сделать это, проверьте один или несколько флажков в соответствующих столбцах **Installation** или **Virus Definition**. **ANY** означает, что вы хотите проверить для любого продукта и любой версии от этого поставщика AV. **Установка** проверяет, установлен ли продукт, и проверки **Определения вируса**, актуальны ли файлы определения вируса на клиенте для указанного продукта.
9. **Нажмите Add Правило**. Новое правило AV добавлено в нижней части **Списка Правила** с названием, которое вы предоставили.

## Создайте требование обновления определения AV

Эти шаги показывают, как создать новое требование Обновления Определения AV для проверки системы клиента для указанных продуктов AV и версий с связанным Правилom AV. Если антивирусные файлы определения клиента не актуальны, пользователь может просто нажать кнопку **Update** на Чистом Агенте Доступа, и Агент заставляет резидентское программное обеспечение AV запускать свой собственный механизм обновления. Обратите внимание на то, что фактический механизм отличается для других продуктов AV, например, оперативных обновлений по сравнению с параметром командной строки.

1. На **Чистой** вкладке **Agent Доступа** щелкните по ссылке подменю **Требований**, и затем **Новому** **Требованию**.

The screenshot shows the 'Device Management > Clean Access' interface. The 'Clean Access Agent' tab is active, and the 'Requirements' sub-tab is selected. The 'New Requirement' form is displayed with the following fields and options:

- Requirement Type:** AV Definition Update
- Do not enforce requirement
- Priority:** 1
- Antivirus Vendor Name:** ANY
- \*Note: Vendors without products supported by this requirement type (EarthLink, Inc., GData Software AG, Microsoft Corp., SOFTWIK, Zone Labs LLC) are not listed in the Antivirus Vendor Name list.
- Requirement Name:** Any\_AV\_UpToDate\_WinXP\_Vista
- Description:** Your Anti-Virus definition files are not up-to-date. Please
- Operating System:**
  - 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
    - Vista Enterprise

**Add Requirement**

If the user has one of the following listed products installed, he/she can use the Update button provided by CCA Agent to update the virus definition file if this requirement fails.

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. Для **Требования Тип** выбирают **AV Definition Update**.
3. **Не принуждает** опцию **требования**, проверен по умолчанию, который определяет требование Обновления Определения AV как **дополнительное**. **Примечание:** Поскольку процесс Windows Update выполняется в фоновом режиме, **не принуждайте требование**, установлен по умолчанию для оптимизации пользовательского опыта. Если вы выбираете загрузку Automatically и устанавливаете опцию, рекомендуется оставить это требование как дополнительное. WSUS принудительное обновление может требовать времени, и запущено и выполнено в фоновом режиме.
4. Выберите **Priority** выполнения для этого требования на клиенте. Высокий приоритет,

такой как 1, означает, что это требование проверено в системе перед всеми другими требованиями и появляется в диалоговых окнах Агента в том заказе. Обратите внимание на то, что, если обязательное требование отказывает, Агент не продолжает мимо той точки, пока не успешно выполняется то требование.

5. Выберите **Antivirus Vendor Name** из раскрывающегося меню. Таблица **продуктов** приводит все версии продукта определения вируса, поддерживаемые для каждой клиентской операционной системы.
6. Для **Названия Требования** введите уникальное имя для определения этого требования файла определения AV в Агенте. Название видимо пользователям на Чистых диалоговых окнах Агента Доступа.
7. В **Поле описания** введите описание требования и инструкций для направления пользователей, которые не в состоянии удовлетворять требование. Для требования Обновления Определения AV необходимо включать инструкции для пользователей для нажатия кнопки **Update** для обновления их систем. Помните эту информацию: **Обновление Определения AV** отображает кнопку **Update** на Агенте. **Обновление Определения AS** отображает кнопку **Update** на Агенте. **Windows Update** отображает кнопку **Update** на Агенте.
8. Проверьте один или больше этих флажков для установки **Операционных систем** для требования: **Windows All** **Windows 2000** **Windows ME** **Windows 98** **Windows XP (Все)** **включая всех правопреемников определенных операционных систем Windows XP** **Windows Vista (Все)** **включая всех правопреемников определенных операционных систем Windows Vista**
9. Нажмите **Add Требование** для добавления требования к Списку Требования.

## [Требование карты к правилам](#)

Как только требование создано и ссылки исправления, и инструкции заданы, сопоставляют требование с правилом или рядом правил. Требование к правилу, сопоставляющее, привязывает ruleset, который проверяет, удовлетворяет ли система клиента требование к действию требований пользователя (Кнопка Agent, инструкции, ссылки) необходимый для системы клиента для соответствия.

1. На **Чистой вкладке Agent Доступа** нажмите подменю **Требований**, и затем откройте форму **Правил Требования**.

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 server yet. For AS Spyware Definition rules, the 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. Из меню **Requirement Name** выберите требование для сопоставления.
3. Проверьте операционную систему для требования в меню **Operating System**. Правила для Выбранного списка Операционной системы заполнены со всеми правилами, доступными для выбранного ОС.
4. Для Правил Определения вируса AV (желтые общие сведения), можно дополнительно настроить CAM, чтобы позволить файлам определения на клиенте быть многими днями, более старыми, чем, что CAM имеет в наличии от Обновлений. См. Правила> Информация Поддержки AS AV для последних дат файла продукта. Это позволяет вам настраивать дрейф в требование так, чтобы, если никакие новые файлы определения вируса не освобождены от поставщика продукта, ваши клиенты могли все еще передать требование. Для этого выполните следующие действия: Проверьте правила Определения вируса AV, позвольте файлу определения быть x днями, более старыми, чем флажок. Введите номер в текстовом поле. По умолчанию 0, который указывает, что дата определения не может быть более старой, чем файл/системная дата. Выберите одну из этих опций: **Последняя дата файла** — Это позволяет клиентскому файлу определения быть более старым, чем дата свежего описания вирусов на CAM к числу дней, которое вы задаете. **Текущая системная дата** — Это позволяет клиентскому файлу определения быть более старым, чем системная дата CAM, когда последнее обновление было выполнено числом дней, вы задаете.
5. Прокрутите страницу вниз и проверьте флажок **Select** рядом с каждым правилом, которое вы хотите привязать к требованию. Правила применены в их порядке очередности, как описано в этой таблице:



<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_Installabon	Win ( XP,2000 )
<input type="checkbox"/>	Lavasoft_Any_Definibon	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. Для **Требований, удовлетворенных, если**, выберите одну из этих опций: Если все правила должны быть удовлетворены для клиента, чтобы быть рассмотренными в соответствии с требованием, **все выбранные правила успешно выполняются** —Если по крайней мере одно выбранное правило должно быть удовлетворено для клиента, чтобы быть рассмотренным в соответствии с требованием, **любое выбранное правило успешно выполняется** —Если выбранные правила должны все быть не в состоянии для клиента быть рассмотренными в соответствии с требованием, **никакое выбранное правило не успешно выполняется** —Если клиенты не в соответствии с требованием, они должны установить программное обеспечение, привязанное к требованию, или завершить обязательные шаги.

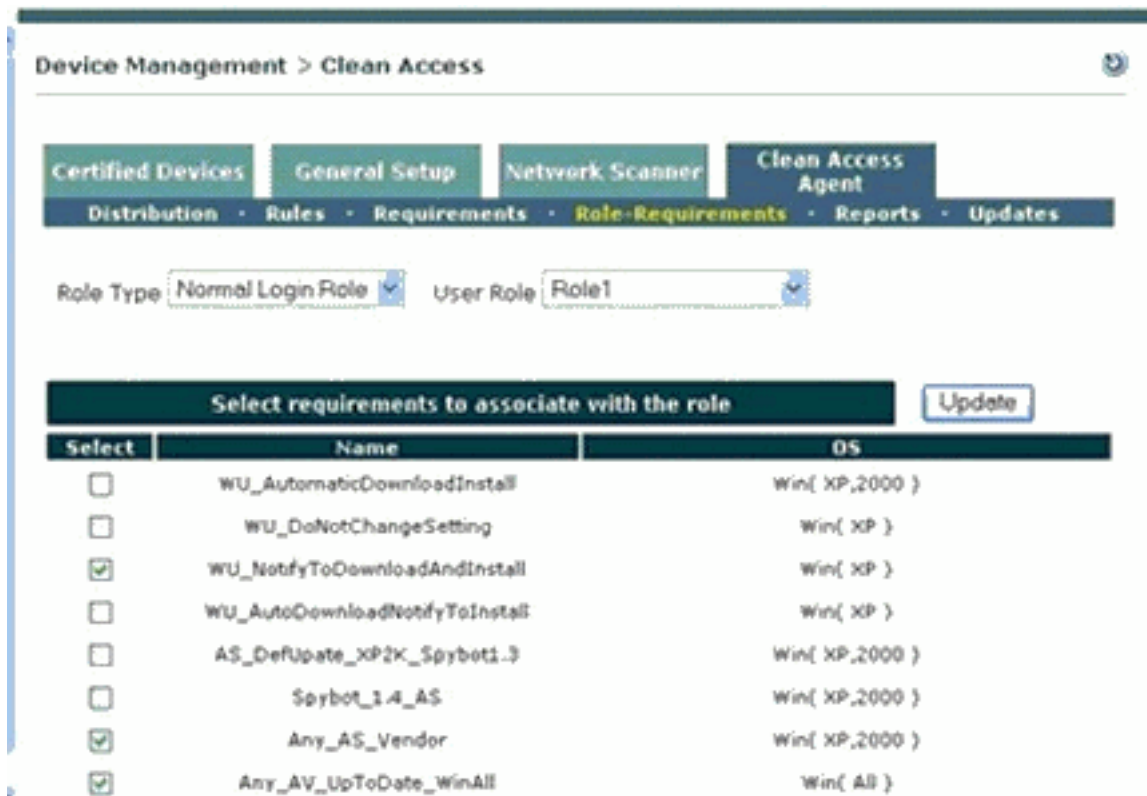
7. Нажмите кнопку **Update (Обновить)**.

## [Примените требования к роли](#)

Как только требования созданы, настроены с шагами исправления и привязаны к правилам, они должны быть сопоставлены с ролями пользователя. Этот шаг применяет ваши требования к группам пользователей в системе.

**Примечание:** Удостоверьтесь, что вам уже создали обычные роли регистрационной информации пользователя для входа.

1. На **Чистой вкладке Agent Доступа** щелкните по ссылке подменю **Требований**





Роли.

2. Из меню **Role Type** выберите тип роли для настройки. В большинстве случаев это - **Обычная Роль Входа в систему**.
3. Выберите название роли из меню **User Role**.
4. Проверьте флажок **Select** для каждого требования, вы хотите примениться к пользователям в роли.
5. **Нажмите кнопку Update (Обновить)**.
6. Перед завершением удостоверьтесь, что пользователи в роли обязаны использовать Чистого Агента Доступа.

## [Проверьте требования](#)

Чистый Access Manager автоматически проверяет требования и правила, поскольку они созданы. Столбец **Validity** под **Управлением устройствами > Чистый Доступ > Чистый Агент Доступа > Требования > Список Требования** отображает законность требования, как показано:

-  — Требование допустимо.
-  — Требование недопустимо. Выделите этот значок со своей мышью в показе заказа сообщение о статусе законности для этого требования. Состояния сообщения о статусе, которые управляют и которые проверяют, заставляют требование быть недопустимым в этом формате: `Invalid rule [rulename] in package [requirementname] (Rule verification error: Invalid check [checkname] in rule expression)`

Требование должно быть исправлено и сделано допустимое, прежде чем оно сможет использоваться. Когда существует несоответствие операционной системы, Как правило, требования и правила становятся недопустимыми.

Для исправления недопустимого требования выполните эти шаги:

1. Выберите **Device Management > Clean Access > Clean Access Agent > Requirements >**

## Requirement-Rules.

- Исправьте любые недопустимые правила или проверки.
- Выберите недопустимое **Название Требования** из раскрывающегося меню.
- Выберите **операционную систему**.
- Удостоверьтесь **Требование, удовлетворенное если**: выражение правильно настроено.
- Удостоверьтесь, что правила, выбранные для требования, допустимы, что означает, что у них есть синяя метка выбора в столбце Validity.



Status message for invalid requirement

## Правила Cisco

Правило является условным оператором, составленным из одной или более проверок. Объединения правила сверяются с логическими операторами для формирования булева оператора, который может протестировать множественные функции системы клиента.

Устройство Cisco NAC предоставляет ряд предварительно сконфигурированных правил и посылает багажом ссылку Обновлений. Предварительно сконфигурированные правила имеют префикс `pr` на их названия, такие как `pr_AutoUpdateCheck_Rule`. Посмотрите [Cisco Предварительно сконфигурированные Правила \("PR "\)](#) для получения дополнительной информации.

## Проверки Cisco

Проверка является условным оператором, который исследует функцию системы клиента, такой как файл, ключ реестра, сервис или приложение. Предварительно сконфигурированные проверки имеют префикс `pc` на их названия, такие как `pc_Hotfix828035`. Эта таблица приводит типы доступных проверок и что они тестируют.

Проверьте категорию	Проверьте тип
Проверка реестра	<ul style="list-style-type: none"><li>существует ли ключ реестра</li><li>значение ключа реестра</li></ul>
Проверка файла	<ul style="list-style-type: none"><li>существует ли файл</li></ul>

	<ul style="list-style-type: none"> <li>• дата модификации или создания</li> <li>• версия файла</li> </ul>
Сервисная проверка	<ul style="list-style-type: none"> <li>• выполняется ли сервис</li> </ul>
Проверка приложения	<ul style="list-style-type: none"> <li>• действительно ли выполнение приложения</li> </ul>

## [Cisco предварительно сконфигурированные правила \(“PR\\_”\)](#)

Устройство Cisco NAC предоставляет ряд предварительно сконфигурированных правил и проверок, которые загружены к CAM через страницу **Updates** на вебе - консоли CAM под **Управлением устройствами> Чистый Доступ> Чистый Агент Доступа> Обновления**.

Предварительно сконфигурированные правила имеют префикс `pr` на их названия, например `pr_XP_Hotfixes`, и могут быть скопированы для использования в качестве шаблона, но не могут быть отредактированы или удалены. Можно нажать **кнопку Edit** для любого правила `pr_` для просмотра выражения правила, которое определяет его. Выражение правила для предварительно сконфигурированного правила составлено из предварительно сконфигурированных проверок, таких как `pc_Hotfix835732` и булевы операторы. Выражение правила для предварительно сконфигурированных правил обновлено посредством Обновлений Cisco. Например, когда новые Важные заплатки Операционной системы Windows освобождены для Windows XP, правило `pr_XP_Hotfixes` обновлено со связанными проверками заплатки.

Предварительно сконфигурированные правила перечислены под **Управлением устройствами> Чистый Доступ> Чистый Агент Доступа> Правила> Список Правила**. Предварительно сконфигурированные проверки имеют префикс `pc` на их названия и перечислены под **Управлением устройствами> Чистый Доступ> Чистый Агент Доступа> Правила> Список проверки**.

**Примечание:** Предварительно сконфигурированные правила Cisco предназначены для оказания поддержки для Важных заплат Операционной системы Windows только.

## [Устранение неполадок](#)

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

### [Cisco Clean Access не обновляет определение AV для клиентов](#)

Для устранения указанной неполадки выполните следующие действия:

1. В CAM выберите **Device Management> Clean Access> Requirements> Requirement-Rules**.
2. Отмените выбор предварительно сконфигурированных правил (`pr_`), если таковые имеются.
3. Выберите соответствующие правила AV.

### [ССА, неспособный обнаружить AV](#)

Если вы подозреваете, что CCA не обнаруживает или распознает определенные проверки AV, необходимо выполнить инструмент диагностики OESIS в клиенте.

Выполните следующие действия:

1. Enable logging. См. [Включают Ведение журнала отладки на Чистом Агенте Доступа](#) для инструкций по тому, как включить ведение журнала отладки на клиенте.
2. Попробуйте войти.
3. Выполните инструмент диагностики OESIS.
4. Отключите регистрацию.

**Примечание:** Если можно захватить экспорт структуры ключа реестра от продукта AV, обычно расположенного в HKLM\Software \<av\_vendor>, который полезен также.

## [Дополнительные сведения](#)

- [Страница технической поддержки устройства Cisco NAC \(Clean Access\)](#)
- [Cisco Systems – техническая поддержка и документация](#)