

# Проблема входа в систему Cisco NAC Appliance (Clean Access)

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Проблема 1](#)

[Решение](#)

[Проблема 2](#)

[Решение](#)

[Проблема 3](#)

[Решение](#)

[Проблема 4](#)

[Решение](#)

[Проблема 5](#)

[Решение](#)

[Проблема 6](#)

[Решение](#)

[Дополнительные сведения](#)

## Введение

Этот документ описывает проблему приглашения регистрации устройства Cisco NAC (Clean Access) для нескольких пользователей, которые пытаются войти в систему общего компьютера.

## Предварительные условия

### Требования

Для этого документа отсутствуют особые требования.

### Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

## Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

## Проблема 1

Чистый сервер доступа (CAS) покрывает несколько пользователей, которые пытаются получить доступ от общего компьютера. Когда входы пользователя в систему в через веб-портал к CAS и затем выходят из системы, эта проблема происходит. Когда следующий пользователь использует тот же общий компьютер для входа в систему, приглашение не появляется.

## Решение

Для устранения указанной неполадки выполните следующие действия:

1. От вашего Менеджера Cisco Clean Access (CAM) выберите **Device Management> Clean**



**Access> General Setup.**

2. Нажмите **Web Login** и выберите роль пользователя из выпадающего списка Роли пользователя. Данный пример использует *Role1*.

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

**Web Login** · Agent Login

User Role

Operating System

Use 'All' settings for the WINDOWS OS family if no version-specific settings are specified

Show [Network Scanner User Agreement page](#) to web login users

Enable pop-up scan vulnerability reports from User Agreement page

Require users to be certified at every web login

Exempt certified devices from web login requirement by adding to MAC filters

Block/Quarantine users with [vulnerabilities](#) in role:

Show quarantined users User Agreement Page of:

3. Удостоверьтесь что, если Операционная система установлена в **WINDOWS ALL**, что у вас также есть **Использование параметры настройки ALL для семейства ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS**, если никакие специфичные для версии параметры настройки не заданы выбранные.
4. Нажмите флажок для **Требуют, чтобы пользователи сертифицировались при каждом веб-входе в систему**. Этот флажок вынуждает пользователя пройти сеть, просматривая каждый раз, когда они обращаются к сети. **Примечание:** Если отключенный (по умолчанию), пользователи только должны сертифицироваться первоначально, они обращаются к сети, или пока их MAC-адрес не очищен от Сертифицированного Списка.
5. Нажмите кнопку **Update (Обновить)**.

## Проблема 2

Вы могли бы получить эту ошибку при доступе к CAS через webconsole (https):

The link that you requested is not present on this Clean Access System. If you reached this page by following a link from the user interface of the Clean Access Manager or Server, then please report this as a bug.

### Решение

Можно переиздать сертификаты на CAS и CAM для решения этого вопроса.

## Проблема 3

См. информацию в [разделе решения](#), если вы получаете эту ошибку:

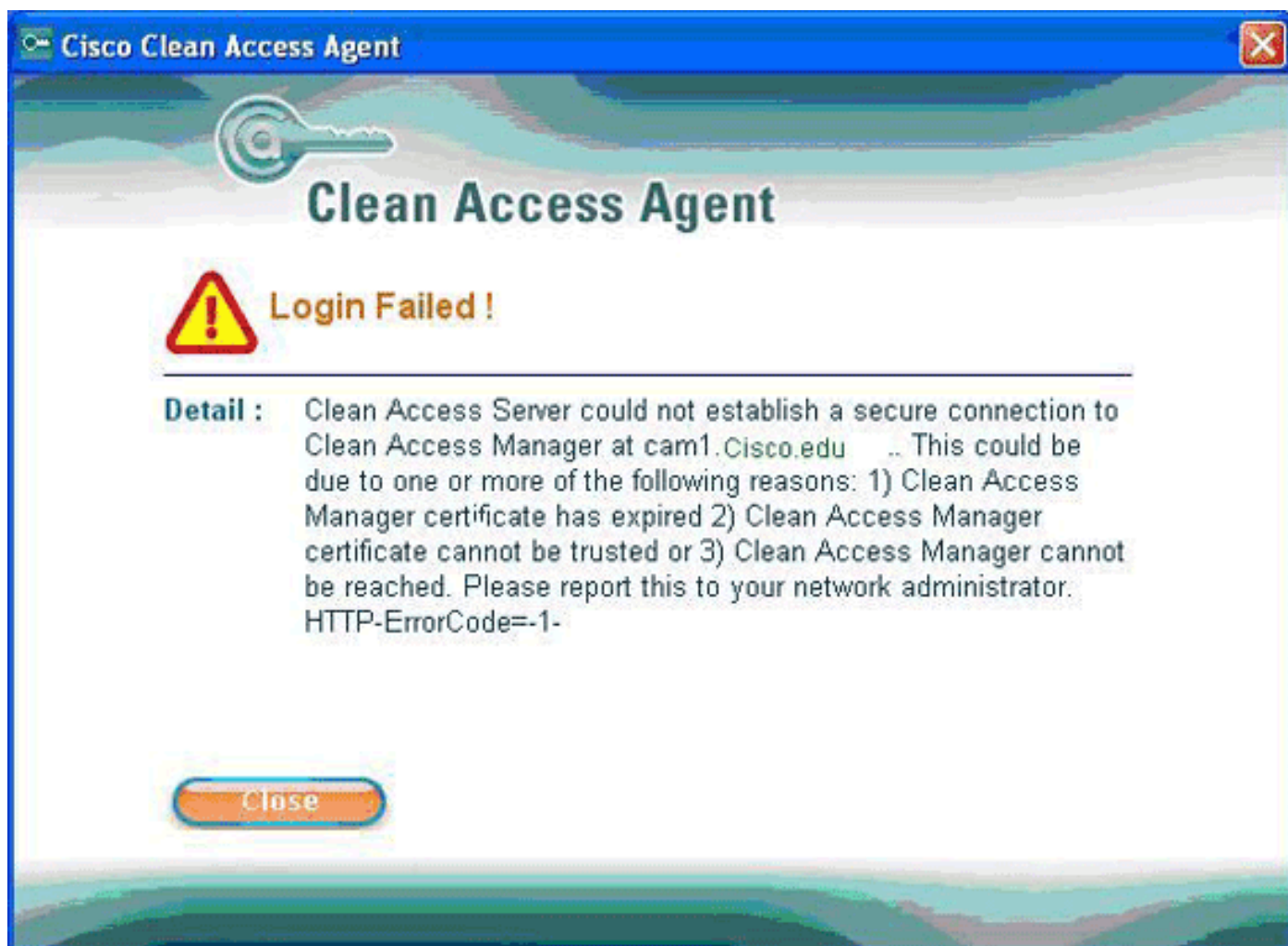
Cisco Clean Access Agent is having problem communicate with NAC appliance server. This could be course by the SSL. Please make sure the certificate on the NAC appliance server is valid (use Domain name and date/time Must not expire). If the NAC Appliance uses the temporary certificate, you have to install the root certificate into the certificate keyChains

## Решение

Эта ошибка замечена на Mac OS в частности. Основная причина для проблемы - то, что сертификат CAS должен быть выполнен к полностью определенному домену или имени хоста, чтобы быть проверенным в MAC OS X, и у клиента должен быть надлежащий корневой сертификат.

## Проблема 4

Вы могли бы получить эту ошибку:



## Решение

Причиной для этого сообщения об ошибках является сертификат SSL, выполненный CAM к имени хоста, которое не мог решить CAS. Можно изменить его на IP-адрес для решения вопроса.

## Проблема 5

NAC мог бы автоматически выйти из системы пользователя после нескольких минут.

## Решение

CAS выходит из системы пользователь, если он не получает пакетов от пользователя на время таймера пульса. Чтобы заставить CAS ждать более длинный период времени, прежде чем он выйдет из системы пользователь, можно установить *таймер пульса* в более высокое значение. Для увеличения долины таймера пульса перейдите к **CAS> Прочее> Таймер пульса**.

## Проблема 6

Вы могли бы получить эту ошибку:

*Ошибка сети! Детальность: ответ сервера не мог быть проанализирован. [12152]*

## Решение

Для устранения указанной неполадки выполните следующие действия:

1. Открытый Internet Explorer.
2. Нажмите **Tools**.
3. Выберите **Internet Options**.
4. Нажмите вкладку **Content**.
5. Нажмите **Clear SSL State**. Этот шаг очищает сертификат для Internet Explorer.
6. Закройте и вновь откройте Internet Explorer, и затем попытайтесь войти снова.

## Дополнительные сведения

- [Cisco NAC Appliance \(Clean Access\)](#)
- [Cisco Systems – техническая поддержка и документация](#)