

NAC (CCA): Исправление ошибок на CAM/CAS после обновления до версии 4.1.6

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Процедура](#)

[Дополнительные сведения](#)

Введение

Этот документ описывает, как закрепить ошибки сертификата на Clean Access Manager (CAM) / Чистый сервер доступа (CAS) с версией 4.1.6.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с процессом обновления для системы контроля доступа к сети Cisco NAC (NAC) Устройство.

Используемые компоненты

Сведения в этом документе основываются на версии 4.1.6 устройства Cisco NAC с CAM/CAS.

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

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

Процедура

Эти ошибки сертификата найдены или в `/perfigo/logs/perfigo-redirect.log0.log.0` или в `/perfigo/logs/perfigo-log0.log.0`.

Вот пример ошибки сертификата:

```
SEVERE: RMISocketFactory:Creating RMI socket failed to host
        10.1.20.10:sun.security.validator.ValidatorException:
        Certificate chaining error
Aug 1, 2008 1:41:22 PM com.perfigo.wlan.web.admin.ConnectorClient connect
SEVERE: Communication Exception : java.rmi.ConnectIOException: Exception
        creating connection to: 10.1.20.10; nested exception is:
        javax.net.ssl.SSLHandshakeException:
        sun.security.validator.ValidatorException: Certificate chaining error
```

Эти ошибки являются результатом улучшений безопасности, сделанных в 4.1.6. В 4.1.6, CAS и действие CAM как клиент и сервер друг другу и должен доверять друг другу. Каждый требует корневых и промежуточных сертификатов от другого. Например, если CAS имеет Сертификат Verisign, и CAM имеет Perfigo (временный) сертификат, и CAS и CAM нужна цепочка Verisign (root и промежуточные звенья) и root Perfigo.

Выполните эти шаги для решения проблемы ошибок сертификата:

1. Выполняют резервное копирование любые установленные сертификаты, которые не являются временными сертификатами. На CAM откройте веб-интерфейс и перейдите к **администрированию > Менеджер CCA > SSL > Сертификат X509**.



The screenshot shows the Cisco Clean Access Standard Manager web interface. The title bar reads "Cisco Clean Access Standard Manager Version 4.1.6". The navigation path is "Administration > Clean Access Manager". The main menu includes "Network", "Failover", "System Time", "SSL", "System Upgrade", "Licensing", and "Support Logs". The "SSL" menu is expanded to show "X509 Certificate" and "Trusted Certificate Authorities". The "X509 Certificate" page is active, displaying a "Choose an action:" dropdown menu with options: "Generate Temporary Certificate", "Export CSR/Private Key/Certificate", and "Import Certificate". Below the dropdown are input fields for "Full Domain Name", "Organization Unit Name", "Organization Name", "City Name", "State Name", and "2-letter Country Code". A "Generate" button is located at the bottom of the form.

На CAS пойдите непосредственно в веб-интерфейс через `https://<IP CAS> / admin`, и затем перейдите к **администрированию > SSL > Сертификат X509**.



Выберите **Export CSR / CSR/Private Key/Certificate** от Выбирания выпадающего списка действия.Нажмите **Export**, расположенный рядом с В настоящее время Устанавливаемым Сертификатом, и сохраните этот файл.Нажмите **Export**, расположенный рядом с В настоящее время Устанавливаемым Секретным ключом, и сохраните этот файл.

- После резервной копии, если CAS и CAM уже не используют временные сертификаты, генерируйте их.На CAM откройте веб-интерфейс и перейдите к **администрированию> Менеджер CCA> SSL> Сертификат X509**.На CAS пойдите непосредственно в веб-интерфейс через <https://<IP CAS> / admin>, и затем перейдите к **администрированию> SSL> Сертификат X509**.Выберите **Generate Temporary Certificate** из выпадающего списка.Заполните поля, перечисленные, и нажмите **Generate**.**Примечание:** Это больше не требует, чтобы перезагрузка вступила в силу.
- Удалите все Доверенные центры сертификации из CAS и CAM. Этот шаг упрощает управлять и улучшать безопасность.На CAM перейдите к **администрированию> Менеджер CCA> SSL> Доверенные центры сертификации**.На CAS перейдите к **администрированию> SSL> Доверенные центры сертификации**.Создайте фильтр для исключения сертификата Perfigo.

X509 Certificate
Trusted Certificate Authorities

▼
Filter
Reset

Browse...
Import
Export

▼

Distinguished Name
 Time

1 2 3 4 5
▶
▶▶
▶▶▶

154 CA(s) - 1 to 10

☐	Distinguished Name	Time Validity	View
<input type="checkbox"/>	EMAILADDRESS=ca@digsigtrust.com, CN=Xcert EZ by DST, O=Xcert EZ by DST, L=Salt Lake City, ST=Utah, C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 1 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 4 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 1 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 4 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 3 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 3 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 2 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 2 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	CN=UTN-USERFirst-Object, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US	yes	

1 2 3 4 5
▶
▶▶
▶▶▶

Выберите **Distinguished Name** из Добавить выпадающего списка фильтра.

X509 Certificate
Trusted Certificate Authorities

Distinguished Name

contains not
 contains
 contains not

Filter

1 2 3 4 5

154 CA(s) - 1 to 10

	Distinguished Name	Time Validity	View
<input type="checkbox"/>	EMAILADDRESS=ca@digsigtrust.com, CN=Xcert E2 by DST, O=Xcert E2 by DST, L=Salt Lake City, ST=Utah, C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 1 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 4 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 1 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 4 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 3 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 3 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 2 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 2 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	CN=UTN-USERFirst-Object, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US	yes	

Выберите **содержит не** от выпадающего списка, который кажется следующим за Составным именем.

X509 Certificate
Trusted Certificate Authorities

Distinguished Name contains not

10
1 2 3 4 5
154 CA(s) - 1 to 10

☐	Distinguished Name	Time Validity	View
<input type="checkbox"/>	EMAILADDRESS=ca@digisigtrust.com, CN=Xcert EZ by DST, O=Xcert EZ by DST, L=Salt Lake City, ST=Utah, C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 1 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 4 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 1 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 4 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 3 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 3 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 2 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 2 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	CN=UTN-USERFirst-Object, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US	yes	

Введите Perfigo в текстовом поле, и затем нажмите Filter.

X509 Certificate Trusted Certificate Authorities

Distinguished Name contains not Perfigo

Add filter... Filter Reset Browse... Import Export

10 Delete Selected 1 2 3 4 5 153 CA(s) - 1 to 10

	Distinguished Name	Time Validity	View
<input type="checkbox"/>	EMAILADDRESS=ca@digsigtrust.com, CN=Xcert EZ by DST, O=Xcert EZ by DST, L=Salt Lake City, ST=Utah, C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 1 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 4 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 1 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 4 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 3 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 3 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 2 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 2 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US	yes	
<input type="checkbox"/>	CN=UTN-USERFirst-Object, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US	yes	

Выберите 100 из выпадающего списка, расположенного рядом с кнопкой Delete Selected. Нажмите флажок ниже Удаления Выбранного выпадающего списка для выбора всех центров сертификации (CAs) в списке. Нажмите **Delete Selected** для удаления всего CAs в списке. Продолжите нажимать коробку и нажимать **Delete Selected**, пока не будут удалены все CAs.

- После удаления всего CAs корневые и промежуточные сертификаты должны быть импортированы. На CAM перейдите к **администрированию > Менеджер CCA > SSL > Доверенные центры сертификации**. На CAS перейдите к **администрированию > SSL > Доверенные центры сертификации**. Нажмите **Browse** и выберите Root Certificate сначала. **Примечание:** Предмет и отправитель должны быть установлены в то же значение. Нажмите **Import**, и CA должен появиться в списке ниже. Выполните ту же процедуру для любых промежуточных сертификатов.
- Установите CAS и сертификаты CAM, что вы выполнили резервное копирование в первом шаге. На CAM откройте веб-интерфейс и перейдите к **администрированию > Менеджер CCA > SSL > Сертификат X509**. На CAS пойдите непосредственно в веб-интерфейс через `https://<IP CAS> / admin`, и затем перейдите к **администрированию > SSL > Сертификат X509**. Выберите **Import Certificate** из выпадающего списка. Нажмите **Browse** и выберите сертификат, сохраненный из шага 1. Нажмите **Upload**. Нажмите **Browse** снова и выберите секретный ключ, который был сохранен от шага 1. Выберите **Private Key** из выпадающего списка Типа файла, и затем нажмите **Upload**. Нажмите **Verify** и **Install Uploaded Certificates**. **Примечание:** Это сообщение об ошибках не быть исправленным этими процедурами: SEVERE: SSLFilter:access deniedCN=cas1.domain.com, OU=Information Technologies, O=Company, ST=State, C=US:Netscape cert type does not permit use for SSL client

Если журналы содержат это сообщение, необходимо связаться с поставщиком

сертификата. Сертификат должен быть переиздан с набором поля Netscape Cert Type и к SSL - серверу и к клиенту SSL.

Дополнительные сведения

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