

# Соединение телефона AnyConnect VPN с примером конфигурации маршрутизатора Cisco IOS

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Настройка](#)

[Топология сети](#)

[Конфигурация сервера VPN SSL](#)

[Шаги обычной конфигурации](#)

[Конфигурация с аутентификацией AAA \(проверка подлинности, авторизация и учет\)](#)

[Конфигурация с логически значимым сертификатом \(LSC\) IP-телефона для аутентификации клиента](#)

[Конфигурация Call Manager](#)

[Экспортируйте самоподписанный или сертификат идентификации от маршрутизатора до CUCM](#)

[Настройте шлюз VPN, группу и профиль в CUCM](#)

[Примените группу и профиль к IP-телефону с общим телефонным профилем](#)

[Примените общий телефонный профиль к IP-телефону](#)

[Установите логически значимые сертификаты \(LSC\) на Cisco IP Phone](#)

[Зарегистрируйте телефон к Call Manager снова для загрузки новой конфигурации](#)

[Проверка](#)

[Проверка маршрутизатора](#)

[Проверка CUCM](#)

[Устранение неполадок](#)

[Отладки на сервере VPN SSL](#)

[Отладки с телефона](#)

[Связанные дефекты](#)

## Введение

Этот документ описывает, как настроить маршрутизатор Cisco IOS® и устройства Call Manager так, чтобы Cisco IP Phone могли установить VPN-подключения к маршрутизатору Cisco IOS. Эти VPN-подключения необходимы для обеспечения связи с любым из этих двух методов аутентификации клиента:

- Аутентификация, авторизация и учет (AAA) или локальная база данных
- Телефонный сертификат

# Предварительные условия

## Требования

Для этого документа отсутствуют особые требования.

## Используемые компоненты

Сведения в документе приведены на основе данных версий аппаратного и программного обеспечения:

- Cisco IOS 15.1 (2) T или позже
- Набор функций / Лицензия: Universal (Данные и Security & UC) для маршрутизатора с интеграцией служб (ISR) Cisco IOS-G2
- Набор функций / Лицензия: Дополнительная безопасность для ISR Cisco IOS
- Выпуск 8.0.1.100000-4 Cisco Unified Communications Manager (CUCM) или позже
- Выпуск 9.0 (2) SR1S IP-телефона - протокол SCCP или позже

Для полного списка поддерживаемых телефонов в вашей версии CUCM выполните эти шаги:

1. Откройте этот URL: <https://<IP-адрес сервера CUCM>:8443/cucreports/systemReports.do>
2. Выберите **Unified CM Phone Feature List> Generate новый отчёт> Функция: Виртуальная частная сеть.**

Версии, используемые в этом примере конфигурации, включают:

- Выпуск 15.1 (4) M4 маршрутизатора Cisco IOS
- Выпуск 8.5.1.10000-26 Call Manager
- Выпуск 9.1 (1) SR1S IP-телефона

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.

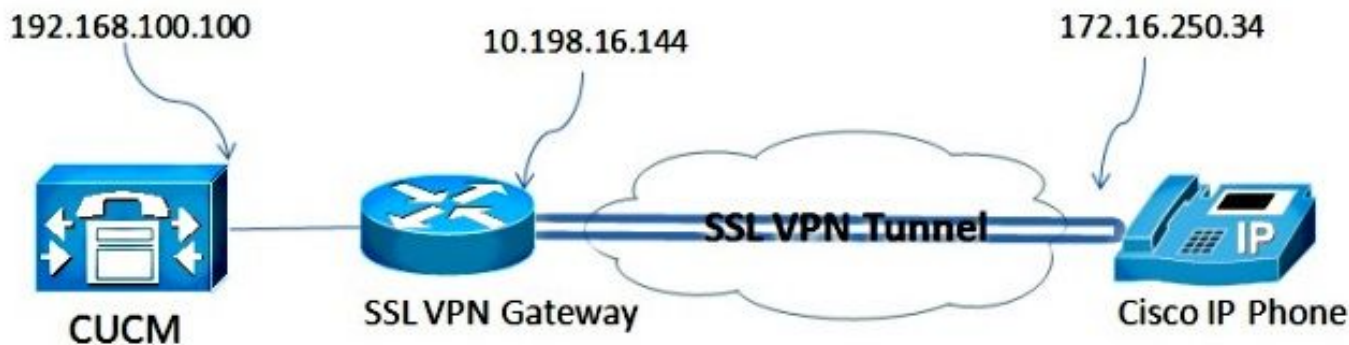
## Настройка

Этот раздел покрывает информацию, необходимую для настройки функций, описанных в этом документе.

**Примечание:** [Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд \(только для зарегистрированных клиентов\).](#)

## Топология сети

Топология, используемая в этом документе, включает один Cisco IP Phone, маршрутизатор Cisco IOS как Шлюз VPN Уровня защищенных сокетов (SSL) и CUCM как голосовой шлюз.



## Конфигурация сервера VPN SSL

В этом разделе описывается настроить головной узел Cisco IOS для разрешения входящих VPN-подключений на базе SSL.

### Шаги обычной конфигурации

1. Генерируйте Ключ Ривест-Шамир-Адлемана (RSA) с длиной 1024 байтов:

```
Router(config)#crypto key generate rsa general-keys label SSL modulus 1024
```

2. Создайте точку доверия для подписанного сертификата и подключите Ключ RSA SSL:

```
Router(config)#crypto pki trustpoint server-certificate
enrollment selfsigned
usage ssl-server
serial-number
subject-name CN=10.198.16.144
revocation-check none
rsa keypair SSL
```

3. Как только точка доверия настроена, зарегистрируйте подписанный сертификат с этой командой:

```
Router(config)#crypto pki enroll server-certificate
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes
```

```
Router Self Signed Certificate successfully created
```

4. Включите корректный пакет AnyConnect на головном узле. Сам телефон не загружает этот пакет. Но без пакета VPN-туннель не устанавливается. Рекомендуется использовать последнюю версию клиентского программного обеспечения, доступную на Cisco.com. Данный пример использует Версию 3.1.3103.

В более старых версиях Cisco IOS это - команда для включения пакета:

```
Router(config)#webvpn install svc flash:anyconnect-win-3.1.03103-k9.pkg
```

Однако в последней версии Cisco IOS, это - команда:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.03103-k9.pkg sequence 1
```

5. Настройте Шлюз VPN. Шлюз WebVPN используется для завершения подключения SSL от пользователя.

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.03103-k9.pkg sequence 1
```

**Примечание:** Или IP-адрес, используемый здесь, должен быть в той же подсети как

интерфейс, с которым телефоны соединяются, или шлюз должен быть получен непосредственно от интерфейса на маршрутизаторе. Шлюз также используется для определения, какой сертификат используется маршрутизатором для проверки себя клиенту.

6. Определите локальный пул, который используется для присвоения IP-адресов на клиентов, когда они соединяются:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.03103-k9.pkg sequence 1
```

## Конфигурация с аутентификацией AAA (проверка подлинности, авторизация и учет)

В этом разделе описываются команды, в которых вы нуждаетесь для настройки AAA-сервера или локальной базы данных для аутентификации телефонов. Если вы планируете использовать аутентификацию только для сертификата для телефонов, продолжиться к следующему разделу.

### Настройте базу данных пользователей

Или Локальная база данных маршрутизатора или внешний AAA-сервер могут использоваться для аутентификации:

- Для настройки локальной базы данных войдите:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.03103-k9.pkg sequence 1
```

- Для настройки удаленного сервера для аутентификации AAA RADIUS войдите:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.03103-k9.pkg sequence 1
```

### Настройте действительный контекст и групповую политику

Действительный Контекст используется для определения атрибутов, которые управляют VPN-подключением, таким как:

- Какой URL использовать, когда вы соединяетесь
- Которые объединяют для использования для присвоения адресов клиента
- Какой метод аутентификации использовать

Эти команды являются примером контекста, который использует аутентификацию AAA (проверка подлинности, авторизация и учет) для клиента:

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.03103-k9.pkg sequence 1
```

## Конфигурация с логически значимым сертификатом (LSC) IP-телефона для аутентификации клиента

В этом разделе описываются команды, в которых вы нуждаетесь для настройки основанной на сертификате аутентификации клиента для телефонов. Однако, чтобы сделать это, знание различных типов телефонных сертификатов требуется:

- **Изготовитель установленный сертификат (MIC)** - MIC включены во все 7941, 7961, и Cisco IP Phone более новой модели. MIC являются 2,048-разрядными ключевыми сертификатами, которые подписаны Центром сертификации (CA) Cisco. Для CUCM для доверия сертификату MIC это использует предварительно установленные сертификаты

CA CAP-RTP-001, CAP-RTP-002 и Cisco\_Manufacturing\_CA в его базе доверенных сертификатов сертификата. Поскольку этот сертификат предоставлен изготовителем сам, как обозначено на название, не рекомендуется использовать этот сертификат для аутентификации клиента.

- **LSC** - LSC защищает соединение между CUCM и телефоном после настройки режима безопасности устройства для аутентификации или шифрования. LSC обладает открытым ключом для Cisco IP Phone, который подписан секретным ключом функции представительства сертифицирующей организации (CAPF) CUCM. Это - более безопасный метод (в противоположность использованию MIC).

**Внимание.** : Из-за риска повышенного уровня безопасности, Cisco рекомендует использование MIC исключительно для установки LSC а не для продолжительного использования. Клиенты, которые настраивают Cisco IP Phone, чтобы использовать MIC для аутентификации Transport Layer Security (TLS), или для любой другой цели, сделать так в их собственном риске.

В этом примере конфигурации LSC используется для аутентификации телефонов.

**Совет:** Самый безопасный способ подключить ваш телефон состоит в том, чтобы использовать двойную аутентификацию, которая комбинирует сертификат и аутентификацию AAA (проверка подлинности, авторизация и учет). Можно настроить это при объединении команд, используемых для каждого под одним действительным контекстом.

## Настройте точку доверия для проверки сертификата клиента

Маршрутизатору нужно было установить сертификат CAPF для проверки LSC от IP-телефона. Чтобы получить тот сертификат и установить его на маршрутизаторе, выполните эти шаги:

1. Перейдите к Административной веб - странице Операционной системы (OS) CUCM.
2. Выберите **Security> Certificate Management**.

**Примечание:** Это местоположение могло бы измениться на основе версии CUCM.

3. Найдите сертификат маркированным **CAPF** и загрузите файл **.pem**. Сохраните его как файл **.txt**
4. Как только certificate извлечено, создайте новую точку доверия на маршрутизаторе и аутентифицируйте точку доверия с CAPF, как показано здесь. Когда предложено для закодированного сертификата CA base64, выберите и вставьте текст в загруженном файле **.pem** наряду с BEGIN и Конечными линиями. Router(config)#**crypto pki trustpoint CAPF**  
enrollment terminal  
authorization username subjectname commonname  
revocation-check none  
Router(config)#**crypto pki authenticate CAPF**  
Router(config)#

```
<base-64 encoded CA certificate>
```

```
quit
```

### Вещи к Примечание:

- Метод регистрации является предельным, потому что сертификат должен быть вручную установлен на маршрутизаторе.

- Команда **authorization username** требуется для сообщения маршрутизатора, что использовать в качестве имени пользователя, когда клиент делает соединение. В этом случае это использует Общее имя (CN).
- Проверка аннулирования должна быть отключена, потому что телефонным сертификатам не определили Список отозванных сертификатов (CRL). Так, пока это не отключено, сбои соединения и отладки Инфраструктуры открытых ключей (PKI)

показывают ЭТИ ВЫХОДНЫЕ ДАННЫЕ:

```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
query CRL.
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilities request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```

## Настройте действительный контекст и групповую политику

Эта часть конфигурации подобна конфигурации, используемой ранее, за исключением двух точек:

- Метод аутентификации
- Точка доверия, которую контекст использует для аутентификации телефонов

Команды показывают здесь:

```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
query CRL.
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilities request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```

## Конфигурация Call Manager

В этом разделе описываются действия настройки Call Manager.

### Экспортируйте самоподписанный или сертификат идентификации от маршрутизатора до CUCM

Чтобы экспортировать сертификат от маршрутизатора и импортировать сертификат в Call

Manager как Телефонный Тростовый VPN сертификат, выполните эти шаги:

1. Проверьте сертификат, используемый для SSL.

```
Router#show webvpn gateway SSL
SSL Trustpoint: server-certificate
```

2. Экспортируйте сертификат.

```
Router(config)#crypto pki export server-certificate pem terminal
The Privacy Enhanced Mail (PEM) encoded identity certificate follows:
-----BEGIN CERTIFICATE-----
```

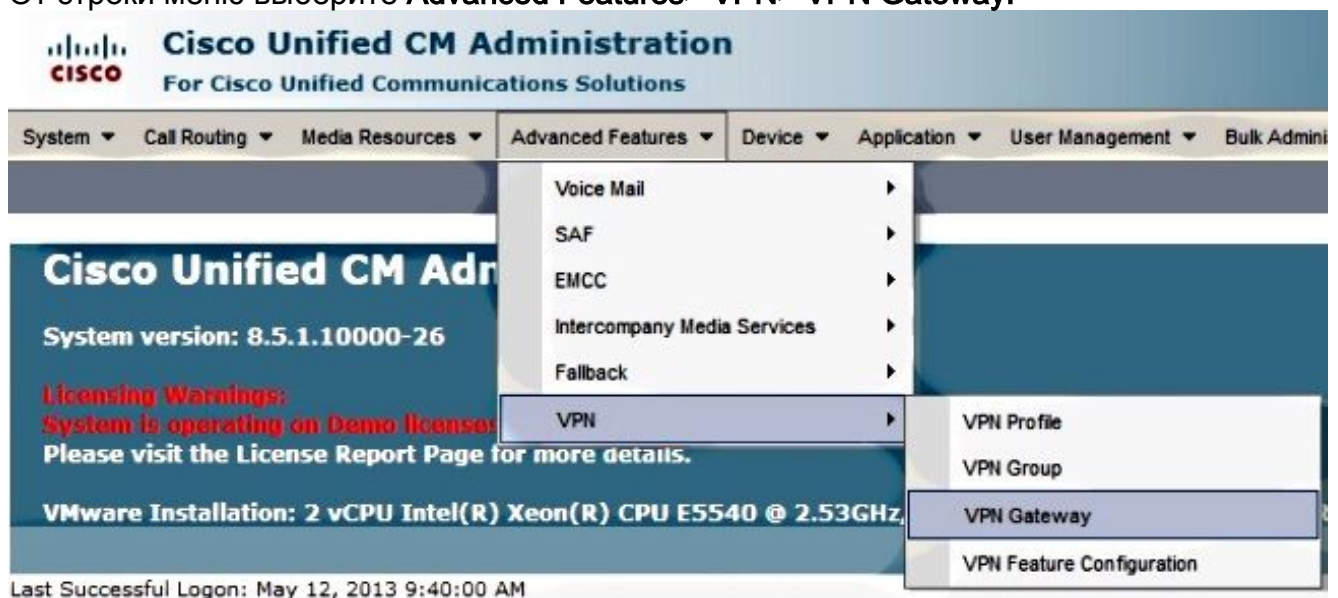
<output removed>

```
-----END CERTIFICATE-----
```

3. Скопируйте текст с терминала и сохраните его как файл .pem.
4. Войдите к Call Manager и выберите **Unified OS Administration> Security> Certificate Management> Upload Certificate> Select Phone-VPN-trust** для загрузки файла сертификата, сохраненного в предыдущем шаге.

Настройте шлюз VPN, группу и профиль в CUCM

1. Переместитесь к Cisco по унифицированному администрированию CM.
2. От строки меню выберите **Advanced Features> VPN> VPN Gateway**.



3. В Окне конфигурации Шлюза VPN выполните эти шаги:  
В Поле имени Шлюза VPN введите имя. Это может быть любым названием. В Поле описания Шлюза VPN введите (дополнительное) описание. В поле VPN Gateway URL введите URL группы, определенный в маршрутизатор. В Сертификатах VPN в этом поле Location выберите сертификат, который был загружен к Call Manager ранее для перемещения его от базы доверенных сертификатов до этого местоположения.

**-VPN Gateway Information-**

VPN Gateway Name\*

VPN Gateway Description

VPN Gateway URL\*

---

**-VPN Gateway Certificates-**

VPN Certificates in your Truststore

SUBJECT: CN=10.198.16.136,unstructuredName=10.198.16.136 ISSUER: CN=10.198.16.136,unstructuredName=10.198.16.136  
SUBJECT: unstructuredName=ASA5520-C.cisco.com,CN=ASA5520-C.cisco.com ISSUER: DC=com,DC=crtac,DC=cisco.com  
SUBJECT: C=CR,O=Cisco,OU=VPN,CN=ASA5520-C.cisco.com,unstructuredName=ASA5520-C.cisco.com ISSUER: CN=10.198.16.140:8443  
SUBJECT: CN=10.198.16.140:8443 ISSUER: CN=10.198.16.140:8443 S/N: e7:e2:72:4f  
SUBJECT: CN=ASA5510-F-IP-PHONE,unstructuredName=ASA5510-F.cisco.com ISSUER: CN=ASA5510-F-IP-PHONE

VPN Certificates in this Location\*

SUBJECT: CN=10.198.16.144,SERIALNUMBER=FTX1309A406+unstructuredName=R2811.vpn.cisco-tac.com ISSUER: CN=10.198.16.144,SERIALNUMBER=FTX1309A406

Save Delete Copy Add New

4. От строки меню выберите **Advanced Features> VPN> VPN Group**.

System Call Routing Media Resources **Advanced Features** Device Application User Management Bulk Administration

**VPN Gateway Configuration**

Save Delete Copy Add

**Status**

Status: Ready

**VPN Gateway Information**

VPN Gateway Name\*

VPN Gateway Description

VPN Gateway URL\*

Voice Mail  
SAF  
EMCC  
Intercompany Media Services  
Fallback  
**VPN**  
VPN Profile  
**VPN Group**  
VPN Gateway  
VPN Feature Configuration

5. В поле All Available VPN Gateways выберите **VPN Gateway**, ранее определенный. Нажмите стрелку вниз для перемещения выбранного шлюза в Выбранные Шлюзы VPN в этом поле VPN Group.



### VPN Group Configuration

Save Delete Copy Add New

---

**Status**

Status: Ready

---

**VPN Group Information**

VPN Group Name\*

VPN Group Description

---

**VPN Gateway Information**

All Available VPN Gateways

Selected VPN Gateways in this VPN Group\*

Save Delete Copy Add New

6. От строки меню выберите **Advanced Features> VPN> VPN Profile**.

System ▾ Call Routing ▾ Media Resources ▾ **Advanced Features ▾** Device ▾ Application ▾ User Management ▾ Bulk Adminis

**VPN Group Configuration**

Save Delete Copy Add

---

**Status**

Status: Ready

---

**VPN Group Information**

VPN Group Name\*

VPN Group Description

- Voice Mail ▸
- SAF ▸
- EMCC ▸
- Intercompany Media Services ▸
- Fallback ▸
- VPN ▸**
  - VPN Profile**
  - VPN Group
  - VPN Gateway
  - VPN Feature Configuration

7. Для настройки Профиля VPN завершите все поля, которые отмечены звездочкой (\*).

## VPN Profile Configuration



Save



Delete



Copy



Add New

### Status



Status: Ready

### VPN Profile Information

Name\*

IOS\_SSL\_Phones

Description

Enable Auto Network Detect

### Tunnel Parameters

MTU\*

1290

Fail to Connect\*

30

Enable Host ID Check

### Client Authentication

Client Authentication Method\* Certificate

Enable Password Persistence

Save

Delete

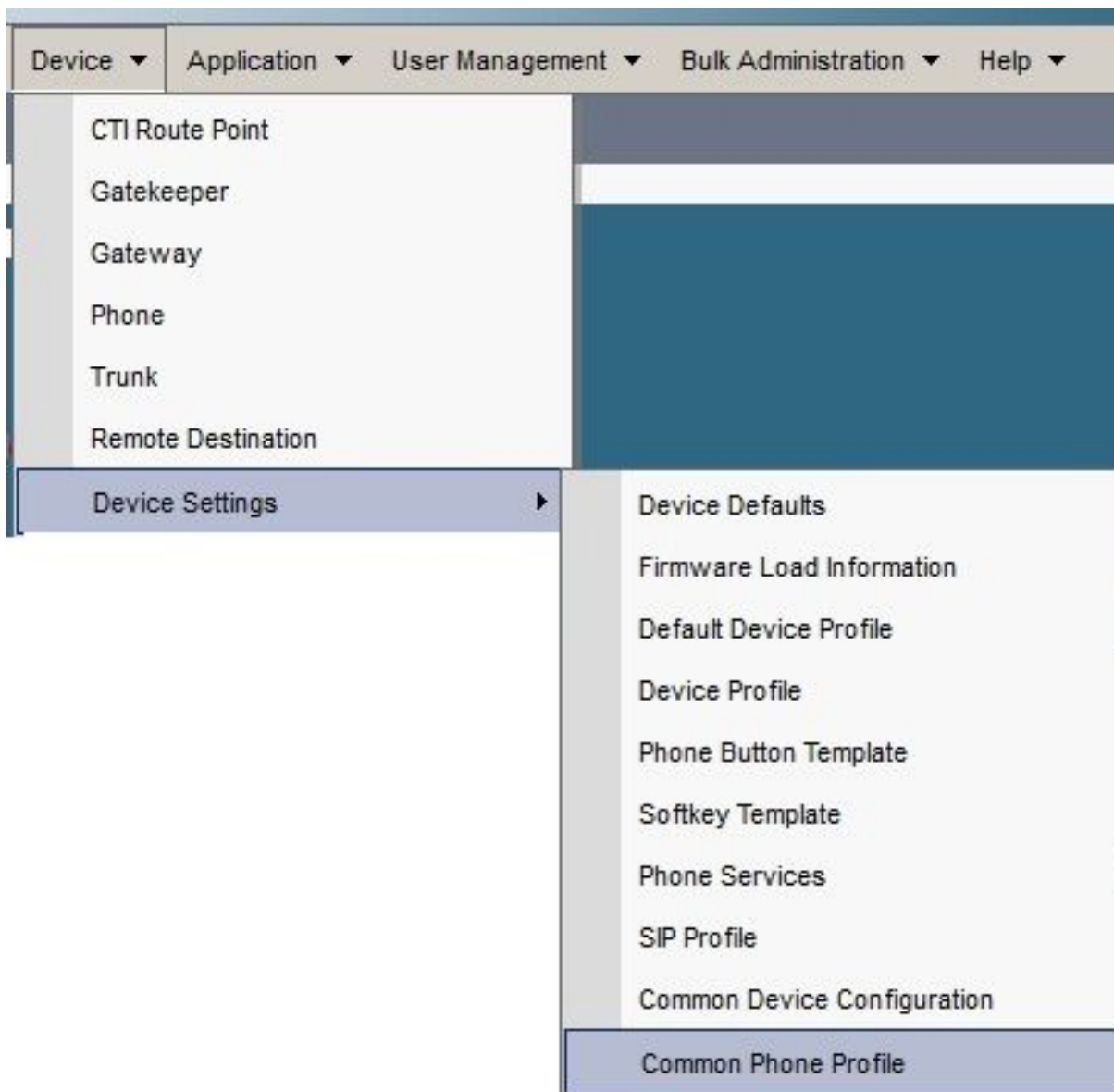
Copy

Add New






**Включите Автоматическую Сеть, Обнаружьте:** Если включено, телефон VPN пропинговывает сервер TFTP. Если никакой ответ не получен, это автоиницирует VPN-подключение. **Включите Проверку Идентификатора хоста:** Если включено, телефон VPN сравнивает Полное доменное имя (FQDN) URL Шлюза VPN против CN/СЕТИ ХРАНЕНИЯ ДАННЫХ (SAN) сертификата. Клиент не в состоянии соединиться, если эти элементы не совпадают или если используется сертификат подстановочного знака со звездочкой (\*). **Устойчивость Enable Password:** Это позволяет телефону VPN кэшировать имя пользователя и пароль для следующей попытки VPN.

Примените группу и профиль к IP-телефону с общим телефонным профилем

В Окне конфигурации Общего телефонного профиля нажмите **Apply Config** для применения новой конфигурации VPN. Можно использовать стандартный **Общий телефонный профиль** или создать новый профиль.



### Common Phone Profile Configuration

Save  Delete  Copy  Reset  Apply Config  Add New

---

#### VPN Information

VPN Group

VPN Profile

Примените общий телефонный профиль к IP-телефону

При создании нового профиля для определенных телефонов/пользователей перейдите к **Окно конфигурации телефона**. В поле Common Phone Profile выберите **Standard Common Phone profile**.



## Установите логически значимые сертификаты (LSC) на Cisco IP Phone

Следующее руководство может использоваться для установки Локально Значительных Сертификатов на Cisco IP Phone. Если аутентификация с помощью LSC используется, этот шаг только необходим. Аутентификация с помощью Manufacturer установленного сертификата (MIC) или имени пользователя и пароля не требует, чтобы был установлен LSC.

[Установите LSC по телефону с набором Режим безопасности Кластера CUCM к Незащищенному.](#)

## Зарегистрируйте телефон к Call Manager снова для загрузки новой конфигурации

Это - заключительный шаг в процессе конфигурирования.

## Проверка

### Проверка маршрутизатора

Для проверки статистики сеанса VPN в маршрутизаторе можно использовать эти команды и проверить различия между выходными данными (выделенными) для имени пользователя и проверки подлинности сертификата:

**Для имени пользователя/проверки подлинности с помощью пароля:**

```
Router#show webvpn session user phones context SSL
Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username : phones           Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
Context : SSL Policy Group : SSLPhones
Last-Used : 00:00:29 Created : 15:40:21.503 GMT
Fri Mar 1 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
```

```

Rekey Time : 3600 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.10.10.1 Netmask : 255.255.255.0
Rx IP Packets : 106 Tx IP Packets : 145
CSTP Started : 00:11:15 Last-Received : 00:00:29
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 51534
DTLS Port : 52768
Router#

```

```
Router#show webvpn session context all
```

```

WebVPN context name: SSL
Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
phones 172.16.250.34 1 00:30:38 00:00:20

```

### Для проверки подлинности сертификата:

```
Router#show webvpn session user SEP8CB64F578B2C context all
```

```

Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

```

```

Username : SEP8CB64F578B2C Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
CA Trustpoint : CAPF
Context : SSL Policy Group :
Last-Used : 00:00:08 Created : 13:09:49.302 GMT
Sat Mar 2 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
Rekey Time : 3600 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.10.10.2 Netmask : 255.255.255.0
Rx IP Packets : 152 Tx IP Packets : 156
CSTP Started : 00:06:44 Last-Received : 00:00:08
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 50122
DTLS Port : 52932

```

```
Router#show webvpn session context all
```





```

WebVPN context name: SSL
Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
SEP8CB64F578B2C 172.16.250.34 1 3d04h 00:00:16

```

## Проверка CUCM

Подтвердите, что IP-телефон зарегистрирован в Call Manager с назначенным адресом маршрутизатор, предоставленный подключению SSL.

Phone (1 - 4 of 4)							
Find Phone where		Device Name	begins with	Find	Clear Filter		
Select item or enter search text							
<input type="checkbox"/>		Device Name(Line) ^	Description	Device Pool	Device Protocol	Status	IP Address
<input type="checkbox"/>		SEP00874338546	Auto 1001	Default	SCCP	Unknown	Unknown
<input type="checkbox"/>		SEP8CB64F576113	Auto 1000	Default	SCCP	Unknown	Unknown
<input type="checkbox"/>		SEP8CB64F578B2C	Auto 1002	Default	SCCP	Registered with 192.168.100.100	10.10.10.5

# Устранение неполадок

## Отладки на сервере VPN SSL

```
Router#show debug
```

```
WebVPN Subsystem:
```

```
WebVPN (verbose) debugging is on
```

```
WebVPN HTTP debugging is on
```

```
WebVPN AAA debugging is on
```

```
WebVPN tunnel debugging is on
```

```
WebVPN Tunnel Events debugging is on
```

```
WebVPN Tunnel Errors debugging is on
```

```
Webvpn Tunnel Packets debugging is on
```

```
PKI:
```

```
Crypto PKI Msg debugging is on
```

```
Crypto PKI Trans debugging is on
```

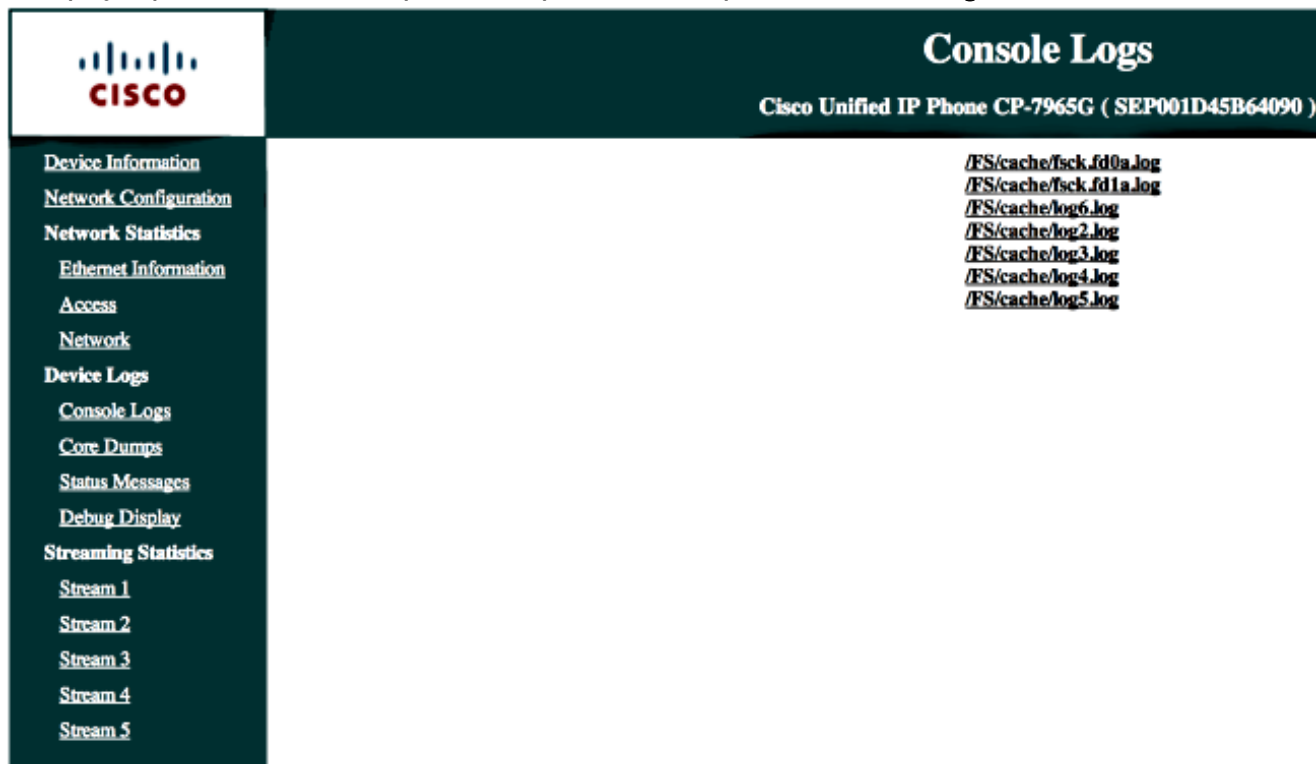
```
Crypto PKI Validation Path debugging is on
```

## Отладки с телефона

1. Перейдите к **Device> Phone** от CUCM.
2. На странице конфигурации устройства, Вебе - доступе набора к **Включенному**.
3. Нажмите **Save**, и затем нажмите **Apply Config**.



4. От браузера введите IP-адрес телефона и выберите **Console Logs** из меню слева.



5. Загрузите все **/FS/cache/log\*.log files.**, файлы console log содержат информацию о том, почему телефон не в состоянии соединиться с VPN.

## Связанные дефекты

Идентификатор ошибки Cisco [CSCty46387](#), IOS SSLVPN: Усовершенствование для имени контекста быть по умолчанию

Идентификатор ошибки Cisco [CSCty46436](#), IOS SSLVPN: Усовершенствование к поведению проверки сертификата клиента