Край совместной работы основанный на TC пример конфигурации оконечных точек

Содержание

Введение

Документ описывает то, что требуется, чтобы настраивать и устранять неполадки Кодека TelePresence (TC) - основанная регистрация оконечной точки через решение для Мобильного и Удаленного доступа.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Решение для мобильного и удаленного доступа
- Сертификаты Сервера Video Communication Server (VCS)
- Скоростная автомагистраль X8.1.1 или позже
- Выпуск 9.1.2 Cisco Unified Communication Manager (CUCM) или позже
- Основанные на TC оконечные точки
- CE8.x требует, чтобы ключ параметра шифрования включил "Край" как опцию инициализации

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- VCS X8.1.1 или позже
- Выпуск 9.1 (2) SU1 CUCM или позже и IM и Присутствие 9.1 (1) или позже
- TC 7.1 или более позднее микропрограммное обеспечение **(рекомендуемый TC7.2)**
- Контроль за VCS и Ядро Скоростной автомагистрали/Скоростной автомагистрали и Край
- CUCM
- Оконечная точка TC

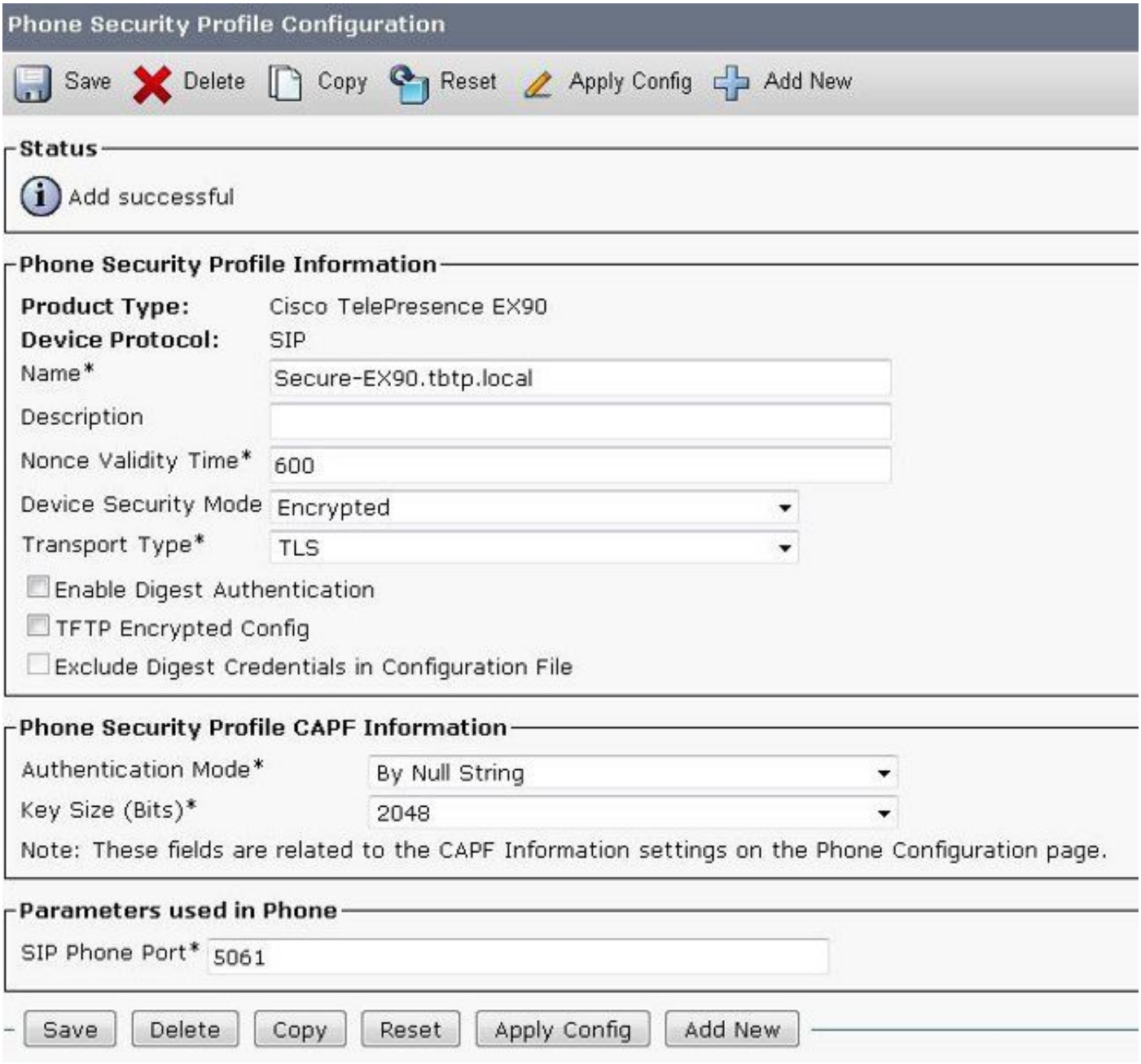
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Эти действия настройки предполагают, что администратор настроит основанную на TC оконечную точку для безопасной регистрации устройства. Безопасная регистрация **НЕ** является требованием, однако полное руководство по решениям Мобильного и Удаленного доступа производит впечатление, которое это - так как существуют снимки экрана от конфигурации, которые показывают безопасные профили устройства на CUCM.

Шаг 1. Создайте безопасный телефонный профиль на CUCM в формате FQDN (Необязательно).

1. В CUCM выберите**> Security System> Телефонный Профиль безопасности**.
2. **Нажмите Добавить нов.**
3. Выберите основанный на TC тип оконечной точки и настройте эти параметры:
4. Название - **безопасный-EX90.tbtp.local (требуемый формат FQDN)**
5. Режим безопасности устройства - **зашифрованный**
6. Тип передачи - **TLS**
7. Порт SIP-телефона - **5061**



Шаг 2. Гарантируйте, что Кластерный Режим безопасности (1) - Смешан (Необязательно).

1. В CUCM выберите **System> Enterprise Parameters**.
2. Прокрутите вниз к **Параметрам безопасности> Кластерный Режим безопасности> 1**.

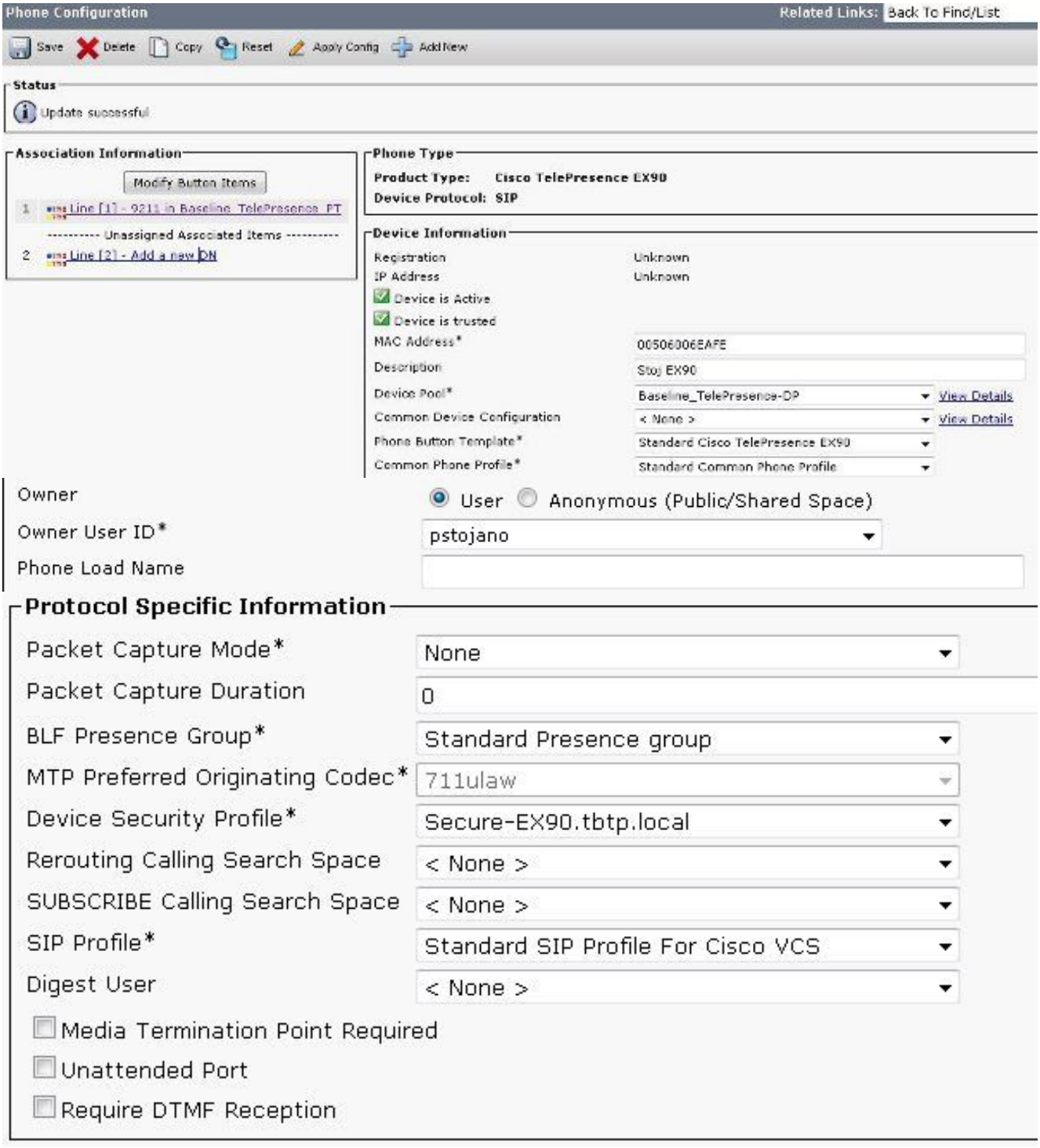
Если значение не 1, CUCM не был защищен. Если это верно, администратор должен рассмотреть один из этих двух документов для обеспечения CUCM.

CUCM 9.1 (2) руководство по обеспечению безопасности

Руководство по обеспечению безопасности CUCM 10

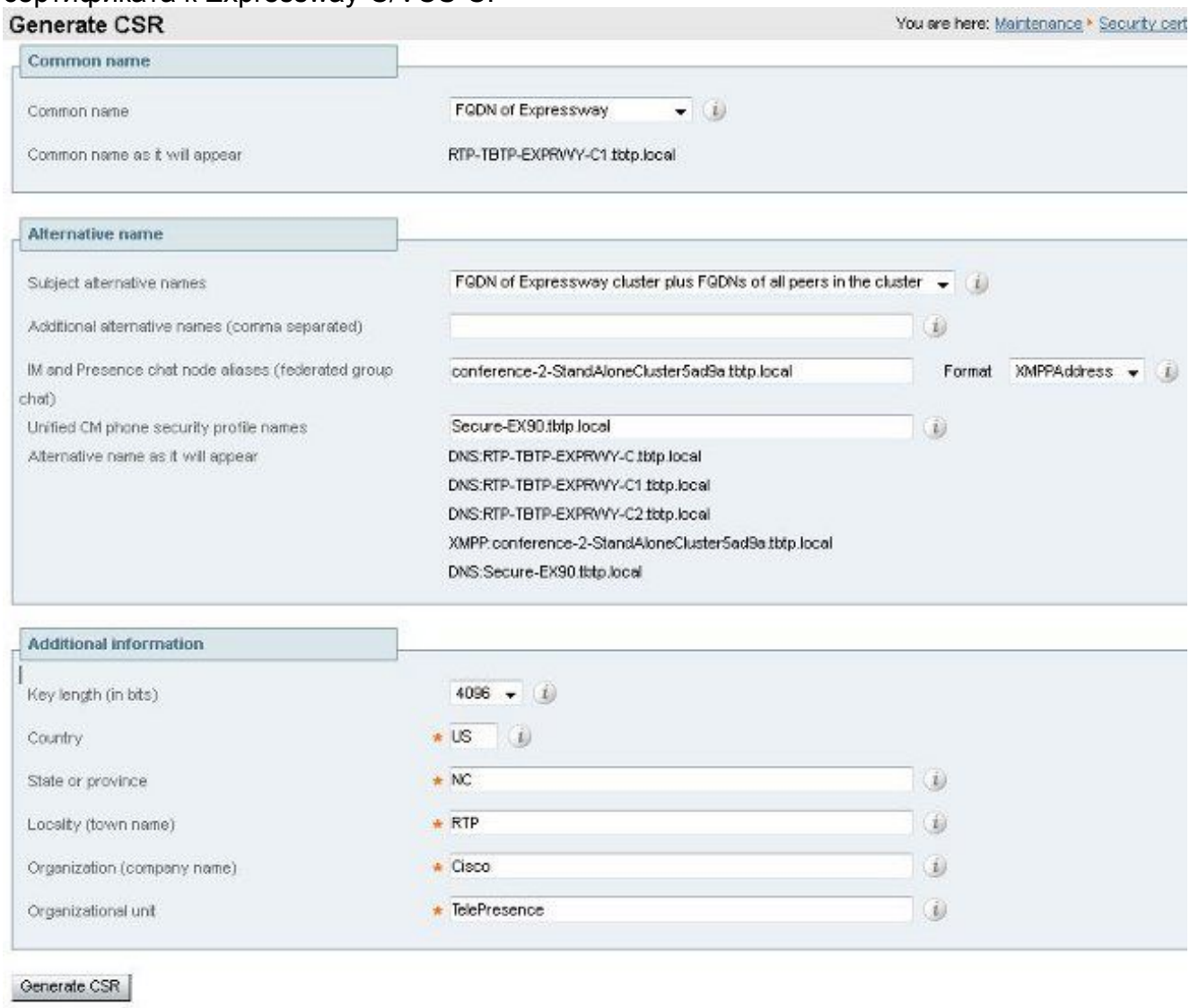
Шаг 3. Создайте профиль в CUCM для основанной на TC оконечной точки.

1. В CUCM выберите **Device> Phone**.
2. **Нажмите Добавить нов.**
3. Выберите основанный на TC тип оконечной точки и настройте эти параметры: MAC-адрес - MAC-адрес от основанного на TC устройстваТребуемые соединенные звездой поля (*)********** OWNER **********-ПользовательПользовательский идентификатор владельца - Владелец связался с устройствомПрофиль безопасности устройства - ранее настроенный профиль (безопасный-EX90.tbtp. лОКАЛЬНЫЙПрофиль SIP - Стандартный профиль SIP или любой пользовательский профиль созданы на предыдущем этапе



Шаг 4. . Добавьте Название Профиля безопасности к SAN Сертификата Expressway-C/VCS-C (Необязательно).

1. В Expressway-C/VCS-C перейдите к **> Security Обслуживания Сертификаты> Серверный сертификат**.
2. Нажмите **Generate CSR**.
3. Заполните поля Certificate Signing Request (CSR) и гарантируйте, что **Унифицированное название профиля безопасности телефона CM** имеет точный Телефонный Профиль безопасности, перечисленный в формате Полного доменного имени (FQDN). Например, **Безопасный-EX90.tbtp. лОКАЛЬНЫЙ. Примечание:** Унифицированные названия профиля безопасности телефона CM перечислены позади поля Subject Alternate Name (SAN).
4. Отошлите CSR или к Внутреннему Центру сертификации (CA) или к Центру сертификации (CA) третьей стороны, который будет подписан.
5. Выберите**> Security Maintenance Сертификаты> Серверный сертификат** для загрузки сертификата к Expressway-C/VCS-C.

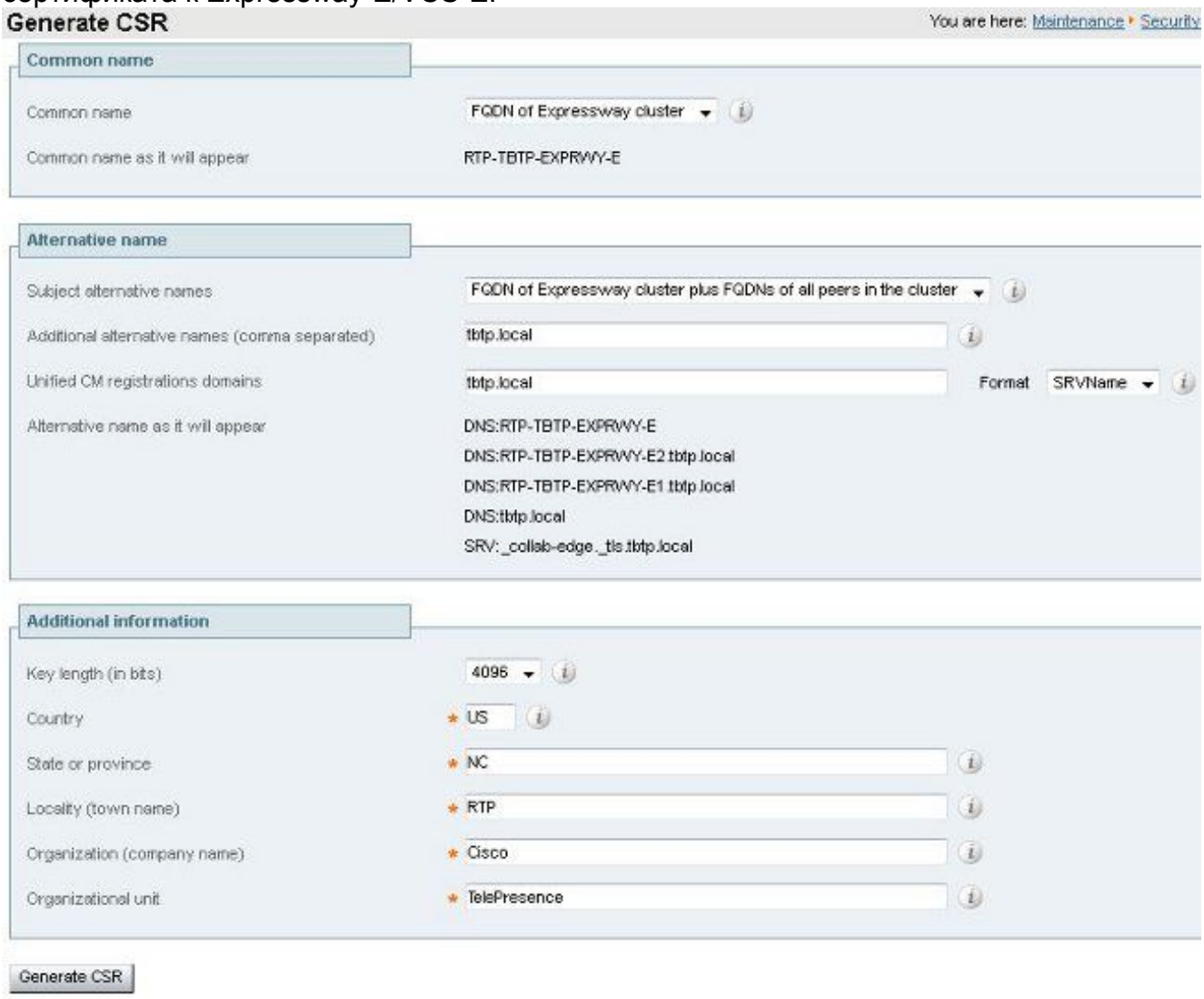


Шаг 5. . Добавьте Домен UC к Сертификату Expressway-E/VCS-E.

1. В Expressway-E/VCS-E выберите**> Security Maintenance Сертификаты> Серверный сертификат**.
2. Нажмите **Generate CSR**.
3. Заполните поля CSR и гарантируйте, что "Объединенные домены Регистраций CM" содержат домен, что основанная на TC оконечная точка сделает Край Совместной

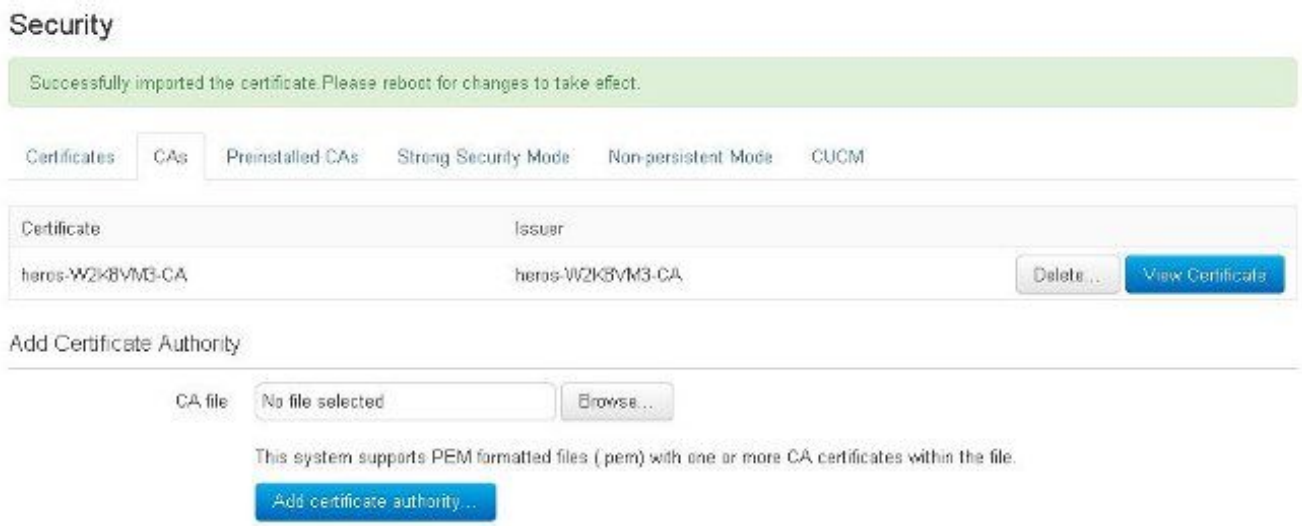
работы (collab-граничными) запросами, или в Сервере доменных имен (DNS) или в Имени сервиса (SRV) форматы.

4. Отошлите CSR или к Внутреннему CA или к CA третьей стороны, который будет подписан.
5. Выберите**> Security Maintenance Сертификаты> Серверный сертификат** для загрузки сертификата к Expressway-E/VCS-E.

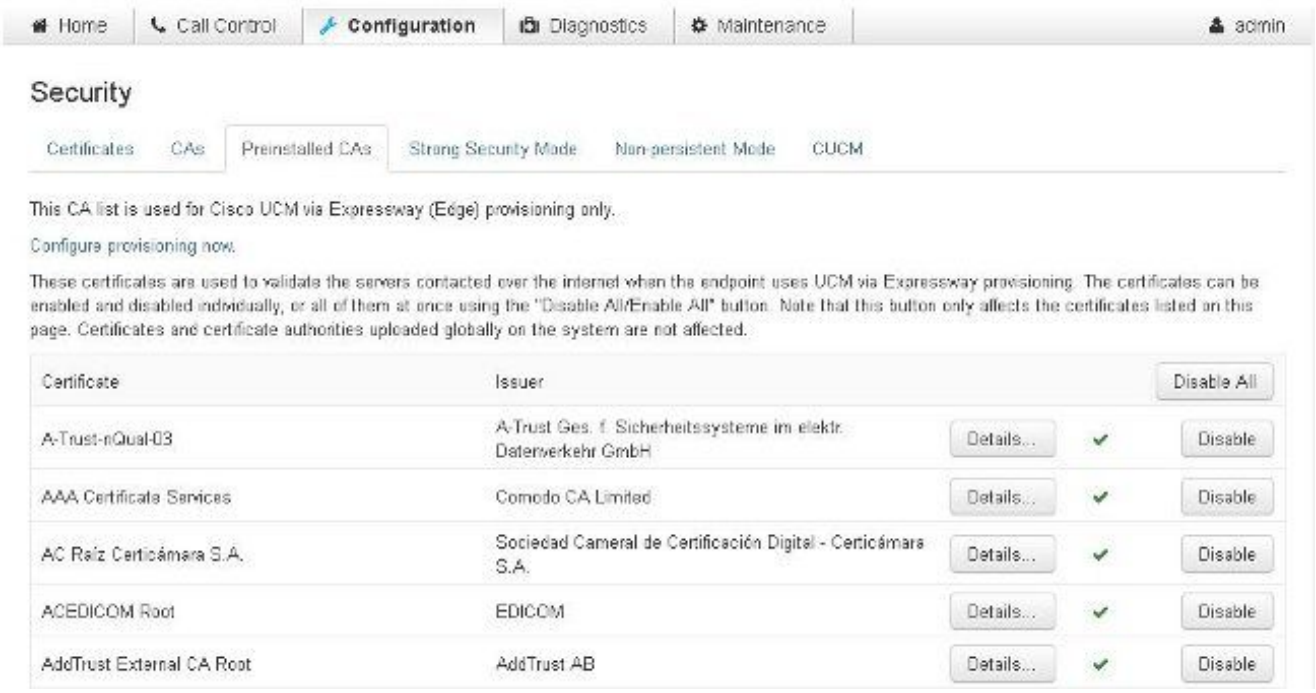


Шаг 6. Установите надлежащий доверенный сертификат CA к основанной на TC оконечной точке.

1. В основанной на TC Оконечной точке выберите**> Security Configuration**.
2. Выберите вкладку **CA** и ищите сертификат CA, который подписал ваш сертификат Expressway-E/VCS-E.
3. **Нажмите Add центр сертификации**. **Примечание:** Как только сертификат успешно добавлен, вы будете видеть, что он перечислил в списке Сертификата.



Примечание: TC 7.2 содержит предварительно установленный список CAs. Если CA, который подписал сертификат Скоростной-автомагистрали-E, содержится в рамках этого списка, шаги, перечисленные в этом разделе, не требуются.



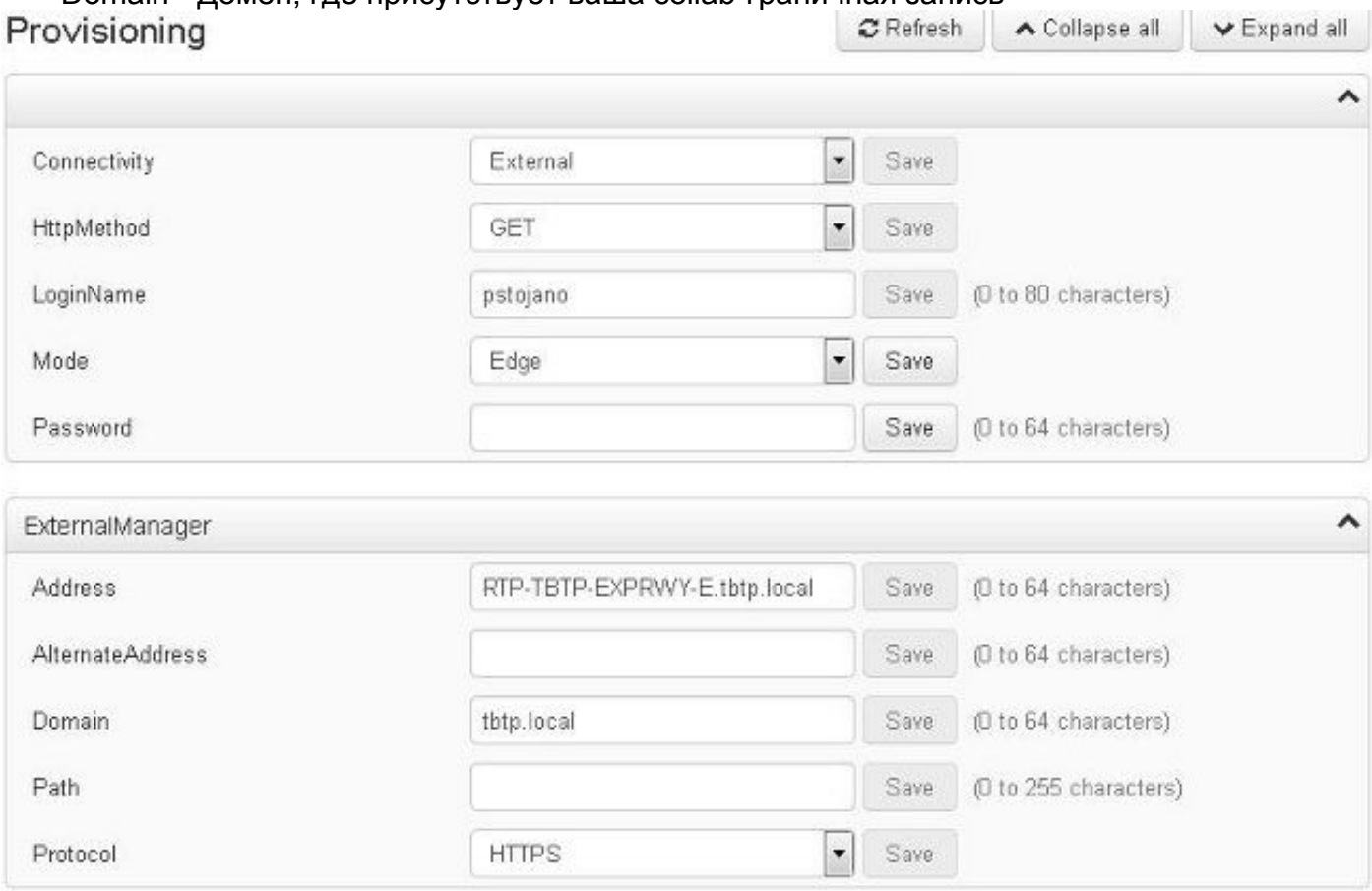
Примечание: Предварительно установленная страница CAs содержит удобную кнопку "Configure provisioning now", которая берет вас непосредственно к требуемой конфигурации, на которую обращают внимание в шаге 2 в следующий раздел.

Шаг 7. Установите основанную на TC оконечную точку для граничной инициализации

- В основанной на TC оконечной точке выберите **Configuration> Network** и гарантируйте, что эти поля должным образом заполнены в под разделом DNS:
  Имя домена
  Адрес сервера

- В основанной на TC оконечной точке выберите **Configuration> Provisioning** и

гарантируйте, что эти поля должным образом заполнены в:
LoginName - как определено в CUCM
Режим- **Край**
Пароль - как определено в CUCM
Внешний менеджер
Адрес - Имя хоста вашего Expressway-E/VCS-E
Domain - Домен, где присутствует ваша collab-граничная запись



Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Основанная на TC оконечная точка

1. В веб-GUI перейдите к "Дом". Ищите 'раздел 1 дюйма прокси SIP для "Зарегистрированного" Статуса. Прокси - адрес является вашим Expressway-E/VCS-E.

2. От CLI введите **xstatus//prov**. Если вы зарегистрированы, необходимо видеть Provisioning status "Provisioned". **xstatus //prov**

```
*s Network 1 IPv4 DHCP ProvisioningDomain: ""
*s Network 1 IPv4 DHCP ProvisioningServer: ""
*s Provisioning CUCM CAPF LSC: Installed
*s Provisioning CUCM CAPF Mode: IgnoreAuth
*s Provisioning CUCM CAPF OperationResult: NotSet
*s Provisioning CUCM CAPF OperationState: NonPending
*s Provisioning CUCM CAPF ServerName: ""
*s Provisioning CUCM CAPF ServerPort: 0
*s Provisioning CUCM CTL State: Installed
*s Provisioning CUCM ExtensionMobility Enabled: False
*s Provisioning CUCM ExtensionMobility LastLoggedInUserId: ""
*s Provisioning CUCM ExtensionMobility LoggedIn: False
*s Provisioning CUCM ITL State: Installed
*s Provisioning CUCM ProvisionSecurity: Signed
*s Provisioning CUCM TVS Proxy 1 IPv6Address: ""
*s Provisioning CUCM TVS Proxy 1 Port: 2445
*s Provisioning CUCM TVS Proxy 1 Priority: 0
*s Provisioning CUCM TVS Proxy 1 Server: "xx.xx.97.131"
*s Provisioning CUCM UserId: "pstojano"
*s Provisioning NextRetry: ""
*s Provisioning Reason: ""
*s Provisioning Server: "xx.xx.97.131"
*s Provisioning Software Current CompletedAt: ""
*s Provisioning Software Current URL: ""
*s Provisioning Software Current VersionId: ""
*s Provisioning Software UpgradeStatus LastChange: "2014-06-30T19:08:40Z"
*s Provisioning Software UpgradeStatus Message: ""
*s Provisioning Software UpgradeStatus Phase: None
*s Provisioning Software UpgradeStatus SecondsUntilUpgrade: 0
*s Provisioning Software UpgradeStatus SessionId: ""
*s Provisioning Software UpgradeStatus Status: None
*s Provisioning Software UpgradeStatus URL: ""
*s Provisioning Software UpgradeStatus VersionId: ""
*s Provisioning Status: Provisioned
** end
```

CUCM

В CUCM выберите **Device> Phone**. Или просмотрите список путем прокрутки или фильтруйте список на основе своей оконечной точки. Необходимо видеть "Зарегистрированный в %CUCM_IP %" сообщение. IP-адрес направо от этого должен быть вашим Expressway-C/VCS-C, который проксирует регистрацию.

Скоростная-автомагистраль-C

- В Expressway-C/VCS-C выберите **Status> Unified Communications> сеансы View Provisioning.**
- Фильтр по IP-адресу вашей основанной на TC оконечной точки. Пример Обеспеченного Сеанса показывают в образе:

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Регистрационные проблемы могут быть вызваны многочисленными факторами, которые включают DNS, проблемы сертификата, конфигурацию, и так далее. Этот раздел включает полный список того, что вы, как правило, видели бы, встречаетесь ли вы с данной проблемой и как повторно добиться его. Если вы сталкиваетесь с проблемами за пределами того, что было уже задокументировано, не стесняйтесь включать его.

Программные средства

Для начинающих, знать о программных средствах в вашем распоряжении.

Оконечная точка TC

Веб-GUI

- all.log
- Запустите расширенная регистрация (включайте перехват полного пакета),

CLI

Эти команды являются самыми выгодными для устранения проблем в режиме реального времени:

- регистрационная отладка ctx HttpClient 9
- регистрируйте ctx отладку ПРОВА 9
- вывод лога на <-Показывает регистрацию через консоль

Эффективный способ для воссоздания проблемы должен переключить Режим конфигурирования от "Края" до "Выключено" и затем назад "Ограничиваться" в веб-GUI. Можно также ввести **xConfiguration Режим конфигурирования:** команда в CLI.

Скоростные автомагистрали

- Журналы диагностики
- TCPDUMP

CUCM

- Трассировки SDI/SDL

Проблема 1: Collab-граничная Запись не Видима, и/или Имя хоста не Разрешимо

Как вы можете видеть get_edge_config отказывает из-за разрешения имен.

Журналы оконечной точки TC

```
15716.23 HttpClient   HTTPClientCurl error
(https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/):
'Couldn't resolve host name'

15716.23 PROV ProvisionRequest failed: 4 (Couldn't resolve host name)
15716.23 PROV I: notify_http_done: Received 0 (Couldn't resolve host name) on request
https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/
```

Исправление

1. Проверьте, присутствует ли collab-граничная запись и возвращает корректное имя хоста.
2. Проверьте, корректна ли информация сервера DNS, настроенная на клиенте.

Проблема 2: CA не присутствует в рамках доверяемого списка CA на основанной на TC оконечной точке

Журналы оконечной точки TC

```
15975.85 HttpClient     Trying xx.xx.105.108...
15975.85 HttpClient Adding handle: conn: 0x48390808
15975.85 HttpClient Adding handle: send: 0
15975.86 HttpClient Adding handle: recv: 0
15975.86 HttpClient Curl_addHandleToPipeline: length: 1
15975.86 HttpClient - Conn 64 (0x48396560) send_pipe: 0, recv_pipe: 0
15975.87 HttpClient - Conn 65 (0x4835a948) send_pipe: 0, recv_pipe: 0
15975.87 HttpClient - Conn 67 (0x48390808) send_pipe: 1, recv_pipe: 0
15975.87 HttpClient Connected to RTP-TBTP-EXPRWY-E.tbtp.local (xx.xx.105.108)
port 8443 (#67)
15975.87 HttpClient successfully set certificate verify locations:
15975.87 HttpClient CAfile: none
CApath: /config/certs/edge_ca_list
15975.88 HttpClient Configuring ssl context with special Edge certificate verifier
15975.88 HttpClient SSLv3, TLS handshake, Client hello (1):
15975.88 HttpClient SSLv3, TLS handshake, Server hello (2):
15975.89 HttpClient SSLv3, TLS handshake, CERT (11):
15975.89 HttpClient SSLv3, TLS alert, Server hello (2):
15975.89 HttpClient SSL certificate problem: self signed certificate in
certificate chain
15975.89 HttpClient Closing connection 67
15975.90 HttpClient HTTPClientCurl error
(https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/):
'Peer certificate cannot be authenticated with given CA certificates'

15975.90 PROV ProvisionRequest failed: 4 (Peer certificate cannot be
authenticated with given CA certificates)
15975.90 PROV I: notify_http_done: Received 0 (Peer certificate cannot be
authenticated with given CA certificates) on request
https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/
15975.90 PROV EDGEProvisionUser: start retry timer for 15 seconds
```

Исправление

1. Проверьте, перечислена ли третья сторона CA под вкладкой **Security> CAs** на оконечной точке.
2. Если CA перечислен, проверьте, что это корректно.

Проблема 3: скоростной-автомагистрали-E не перечислили домен UC в SAN

Журналы оконечной точки TC

```
82850.02 CertificateVerification ERROR: [verify_edge_domain_in_san]: Edge TLS
verification failed: Edge domain 'tbtp.local' and corresponding SRVName
'_collab-edge._tls.tbtp.local' not found in certificate SAN list
82850.02 HttpClient SSLv3, TLS alert, Server hello (2):
82850.02 HttpClient SSL certificate problem: application verification failure
82850.02 HttpClient Closing connection 113
82850.02 HttpClient HTTPClientCurl error
(https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/):
'Peer certificate cannot be authenticated with given CA certificates'
```

SAN скоростной-автомагистрали-E

```
X509v3 Subject Alternative Name:
DNS:RTP-TBTP-EXPRWY-E.tbtp.local, SRV:_collab-edge._tls.tbtppppp.local
```

Исправление

1. Восстановите CSR Скоростной-автомагистрали-E для включения Домена (доменов) UC.
2. Возможно, что на оконечной точке TC параметр **Домена ExternalManager** является "not set" к тому, каков Домен UC. Если это верно, необходимо совпасть с ним.

Проблема 4: Имя пользователя и/или пароль, Предоставленное в Профиле Инициализации TC, Является Неправильным

Журналы оконечной точки TC

```
83716.67 HttpClient     Server auth using Basic with user 'pstojano'
83716.67 HttpClient GET /dGJ0cC5jb20/get_edge_config/ HTTP/1.1
Authorization: xxxxxx
Host: RTP-TBTP-EXPRWY-E.tbtp.local:8443
Cookie: JSESSIONIDSSO=34AFA4A6DEE1DDCE8B1D2694082A6D0A
Content-Type: application/x-www-form-urlencoded
Accept: text/xml
User-Agent: Cisco/TC
Accept-Charset: ISO-8859-1,utf-8
83716.89 HttpClient HTTP/1.1 401 Unauthorized
83716.89 HttpClient Authentication problem. Ignoring this.
83716.90 HttpClient WWW-Authenticate: Basic realm="Cisco-Edge"
83716.90 HttpClient Server CE_C ECS is not blacklisted
83716.90 HttpClient Server: CE_C ECS
83716.90 HttpClient Date: Thu, 25 Sep 2014 17:42:51 GMT
83716.90 HttpClient Age: 0
83716.90 HttpClient Transfer-Encoding: chunked
83716.91 HttpClient Connection: keep-alive
83716.91 HttpClient
83716.91 HttpClient 0
83716.91 HttpClient Connection #116 to host RTP-TBTP-EXPRWY-E.tbtp.local
left intact
83716.91 HttpClient HTTPClientCurl received HTTP error 401

83716.91 PROV ProvisionRequest failed: 5 (HTTP code=401)
83716.91 PROV I: notify_http_done: Received 401 (HTTP code=401) on request
https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/
```

Expressway-C/VCS-C

```
2014-09-25T13:46:20-04:00 RTP-TBTP-EXPRWY-C edgeconfigprovisioning
UTCTime="2014-09-25 17:46:20,92" Module="network.http.edgeconfigprovisioning"
Level="DEBUG" Action="Received"
Request-url="https://xx.xx.97.131:8443/cucm-uds/user/pstojano/devices"
HTTPMSG:
|HTTP/1.1 401 Unauthorized
Expires: Wed, 31 Dec 1969 19:00:00 EST
Server:
Cache-Control: private
Date: Thu, 25 Sep 2014 17:46:20 GMT
Content-Type: text/html;charset=utf-8
WWW-Authenticate: Basic realm="Cisco Web Services Realm"

2014-09-25T13:46:20-04:00 RTP-TBTP-EXPRWY-C UTCTime="2014-09-25 17:46:20,92"
Module="developer.edgeconfigprovisioning.server" Level="DEBUG"
CodeLocation="edgeprotocol(1018)" Detail="Failed to authenticate user against server"
Username="pstojano" Server="('https', 'xx.xx.97.131', 8443)"
Reason="<twisted.python.failure.Failure <type 'exceptions.Exception'>>
"2014-09-25T13:46:20-04:00 RTP-TBTP-EXPRWY-C edgeconfigprovisioning:
Level="INFO" Detail="Failed to authenticate user against server" Username="pstojano"
Server="('https', 'xx.xx.97.131', 8443)" Reason="<twisted.python.failure.Failure
<type 'exceptions.Exception'>>" UTCTime="2014-09-25 17:46:20,92"
```

Исправление

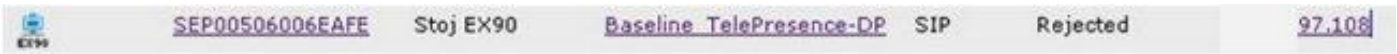
1. Проверьте, что Имя пользователя/Пароль, введенное под страницей Provisioning в оконечную точку TC, допустимо.
2. Проверьте учетные данные против базы данных CUCM.
3. Версия 10 - использует Сам Портал Ухода
4. Версия 9 - использует Параметры пользователя CM

URL для обоих порталов является тем же: **https://%CUCM %/ucmuser/**

Если предоставлено недостаточную ошибку прав, гарантируйте, что эти роли назначены на пользователя:

- Стандартный CTI включен
- Типичный конечный пользователь CCM

Проблема 5: основанная на TC регистрация оконечной точки отклонена



Трассировки CUCM

```
08080021.043 |16:31:15.937 |AppInfo  |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate, Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local,
Expected=SEP00506006EAFE. Will check SAN the next
08080021.044 |16:31:15.937 |AppInfo |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate Error , did not find matching SAN either,
Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local, Expected=Secure-EX90.tbtp.local
08080021.045 |16:31:15.937 |AppInfo |ConnectionFailure - Unified CM failed to open
a TLS connection for the indicated device Device Name:SEP00506006EAFE
IP Address:xx.xx.97.108 IPV6Address: Device type:584 Reason code:2 App ID:Cisco
CallManager Cluster ID:StandAloneCluster Node ID:RTP-TBTP-CUCM9 08080021.046
|16:31:15.938 |AlarmErr |AlarmClass: CallManager, AlarmName: ConnectionFailure,
AlarmSeverity: Error, AlarmMessage: , AlarmDescription: Unified CM failed to open
a TLS connection for the indicated device, AlarmParameters:
```

```
DeviceName:SEP00506006EAFE, IPAddress:xx.xx.97.108, IPV6Address:,
DeviceType:584, Reason:2, AppID:Cisco CallManager, ClusterID:StandAloneCluster,
NodeID:RTP-TBTP-CUCM9,
```

Оконечная точка TC

Фактический Expressway-C/VCS-C

```
08080021.043 |16:31:15.937 |AppInfo  |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate, Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local,
Expected=SEP00506006EAFE. Will check SAN the next
08080021.044 |16:31:15.937 |AppInfo |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate Error , did not find matching SAN either,
Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local, Expected=Secure-EX90.tbtp.local
08080021.045 |16:31:15.937 |AppInfo |ConnectionFailure - Unified CM failed to open
a TLS connection for the indicated device Device Name:SEP00506006EAFE
IP Address:xx.xx.97.108 IPV6Address: Device type:584 Reason code:2 App ID:Cisco
CallManager Cluster ID:StandAloneCluster Node ID:RTP-TBTP-CUCM9 08080021.046
|16:31:15.938 |AlarmErr |AlarmClass: CallManager, AlarmName: ConnectionFailure,
AlarmSeverity: Error, AlarmMessage: , AlarmDescription: Unified CM failed to open
a TLS connection for the indicated device, AlarmParameters:
DeviceName:SEP00506006EAFE, IPAddress:xx.xx.97.108, IPV6Address:,
DeviceType:584, Reason:2, AppID:Cisco CallManager, ClusterID:StandAloneCluster,
NodeID:RTP-TBTP-CUCM9,
```

В этом определенном примере журнала ясно, что Expressway-C/VCS-C не содержит Телефонный Профиль безопасности FQDN в SAN. (Безопасный-EX90.tbtp. лОКАЛЬНЫЙ. В Квитировании Transport Layer Security (TLS) CUCM осматривает серверный сертификат Expressway-C/VCS-C. Так как это не находит его в SAN, это бросает полужирную ошибку и сообщает, что Ожидало Телефонный Профиль безопасности в формате FQDN.

Исправление

1. Проверьте, что Expressway-C/VCS-C содержит Телефонный Профиль безопасности в формате FQDN в SAN, он - серверный сертификат.
2. Проверьте, что устройство использует корректный профиль безопасности в CUCM при использовании безопасного профиля в формате FQDN.
3. Это могло также быть вызвано идентификатором ошибки Cisco CSCuq86376. Если это верно, проверьте SAN размер Expressway-C/VCS-C и позицию Телефонного Профиля безопасности в SAN.

Проблема 6: основанные на TC Сбои Инициализации Оконечной точки - Никакой сервер UDS

Эта ошибка должна присутствовать Под **Диагностикой> Устранение проблем** :

```
08080021.043 |16:31:15.937 |AppInfo  |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate, Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local,
Expected=SEP00506006EAFE. Will check SAN the next
08080021.044 |16:31:15.937 |AppInfo |SIPStationD(18400) - validTLSConnection:TLS
```

```
InvalidX509NameInCertificate Error , did not find matching SAN either,
Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local, Expected=Secure-EX90.tbtp.local
08080021.045 |16:31:15.937 |AppInfo |ConnectionFailure - Unified CM failed to open
a TLS connection for the indicated device Device Name:SEP00506006EAFE
IP Address:xx.xx.97.108 IPV6Address: Device type:584 Reason code:2 App ID:Cisco
CallManager Cluster ID:StandAloneCluster Node ID:RTP-TBTP-CUCM9 08080021.046
|16:31:15.938 |AlarmErr |AlarmClass: CallManager, AlarmName: ConnectionFailure,
AlarmSeverity: Error, AlarmMessage: , AlarmDescription: Unified CM failed to open
a TLS connection for the indicated device, AlarmParameters:
DeviceName:SEP00506006EAFE, IPAddress:xx.xx.97.108, IPV6Address:,
DeviceType:584, Reason:2, AppID:Cisco CallManager, ClusterID:StandAloneCluster,
NodeID:RTP-TBTP-CUCM9,
```

Журналы оконечной точки TC

Перейдите к праву видеть ошибки полужирным

```
9685.56 PROV   REQUEST_EDGE_CONFIG:
9685.56 PROV   <?xml version='1.0' encoding='UTF-8'?>
9685.56 PROV   <getEdgeConfigResponse version="1.0"><serviceConfig><service><name>_cisco-phone-
tftp</name><error>NameError</error></service><service><name>_cuplogin</name><error>NameError</er
ror></service><service><name>_cisco-
uds</name><server><priority>1</priority><weight>1</weight><port>8443</port><address>cucm.domain.
int</address></server></service><service><name>tftpServer</name><address></address><address></ad
dress></service></serviceConfig><edgeConfig><sipEdgeServer><server><address>expe.domain.com</add
ress><tlsPort>5061</tlsPort></server></sipEdgeServer><sipRequest><route>&lt;sip:192.168.2.100:50
61;transport=tls;zone-
id=3;directed;lr&gt;</route></sipRequest><xmppEdgeServer><server><address>expe.domain.com</addre
ss><tlsPort>5222</tlsPort></server></xmppEdgeServer><httpEdgeServer><server><address>expe.domain
.com</address><tlsPort>8443</tlsPort></server></httpEdgeServer><turnEdgeServer/><userUdsServer><
server><address></address><tlsPort>8443</tlsPort></server></userUdsServer></edgeConfig></getEdge
ConfigResponse>
9685.57 PROV ERROR: Edge provisioning failed!
url='https://expe.domain.com:8443/ZXUuY2hlZ2cuY29t/get_edge_config/', message='XML didn't
contain UDS server address'
9685.57 PROV  EDGEProvisionUser: start retry timer for 15 seconds
9700.57 PROV I: [statusCheck] No active VcsE, reprovisioning!
```

Исправление

1. Гарантируйте, что существует Профиль сервиса и CTI Сервис UC, привязанный к учетной записи Конечного пользователя, используемой для запроса инициализации оконечной точки через сервисы MRA.

2. Перейдите **admin CUCM> Управление пользователями> Параметры пользователя> Сервис UC** и создайте CTI Сервис UC, который указывает к IP CUCM (т.е. MRA_UC-сервис).

3. Перейдите **admin CUCM> Управление пользователями> Параметры пользователя> Профиль сервиса** и создайте новый профиль (т.е. MRA_ServiceProfile).

4. В новом Профиле сервиса перейдите к нижней части и в разделе Профиля CTI, выберите новый CTI, который Обслуживают UC, вы просто создали (т.е. MRA_UC-сервис), затем нажмите Save.

5. Перейдите **admin CUCM> Управление пользователями> Конечный пользователь** и найдите, что учетная запись пользователя использовала запрашивать инициализацию оконечной точки через сервисы MRA.

6. При **Сервисных Параметрах настройки** того пользователя гарантируйте, что Кластер Дом является проверкой и что Профиль сервиса UC отражает новый Профиль сервиса, который

вы создали (т.е. MRA_ServiceProfile), затем нажмите Save.

7. Может потребоваться несколько минут для репликации. Попытайтесь отключить режим конфигурирования на оконечной точке и возвратить его на несколько минут спустя, чтобы видеть, регистрируется ли теперь оконечная точка.

Дополнительные сведения

- Руководство мобильного и Удаленного доступа
- Руководство создания сертификата VCS
- EX90/EX60, Начинающий работу Руководство
- Руководство администратора CUCM 9.1
- Cisco Systems – техническая поддержка и документация