Шифрование CUCM 11.0 следующего поколения - шифрование в эллиптических кривых

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Общие сведения
Управление сертификатами
Генерация Сертификатов с шифрованием EC
Конфигурация интерфейса командой строки CLI
CTL и файлы ITL:
Функция представительства сертифицирующей организации (CAPF)
Корпоративные параметры шифров TLS
SIP поддержка ECDSA
Защитите диспетчера CTI поддержка ECDSA
Поддержка HTTPS загрузки конфигурации
Энтропия
Дополнительные сведения

Введение

Этот документ описывает введение, конфигурацию Шифрования Next_Generation (NGE) от Cisco Unified Communications Manager (CUCM) 11.0 и позже, для совещания усиленной безопасности и требований к производительности

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Основы Cisco Call Manager Секурити
- Управление сертификатами Cisco Call Manager

Используемые компоненты

Сведения в этом документе основываются на Cisco CUCM 11.0, где edcsa сертификаты только поддерживаются для CallManager (CallManager-EDCSA)

Примечание: CUCM 11.5 и далее поддерживает сертификаты tomcat-EDCSA также

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.

Родственные продукты

Этот документ может также использоваться с этими программными продуктами и версиями, которые поддерживают сертификаты EDCSA:

- IM Cisco и присутствие 11.5
- Cisco Unity Connection 11.5

Общие сведения

Шифрование в эллиптических кривых (ECC) является подходом к криптографии общего ключа на основе алгебраической структуры эллиптических кривых по ограниченным полям. Одно из главных преимуществ по сравнению с криптографией не-ECC является тем же уровнем безопасности, предоставленным ключами меньшего размера.

Общие Критерии предоставляют обеспечение, что характеристики безопасности работают правильно в оцениваемом решении. Это достигнуто посредством тестирования и совещания обширных требований обеспечения документацией.

Принятый и поддерживаемый 26 Странами Во всем мире через Общее расположение распознавания критериев (CCRA)

Выпуск 11.0 Cisco Unified Communications Manager поддерживает сертификаты Алгоритма цифровой подписи эллиптической кривой (ECDSA).

Эти сертификаты более сильны, чем основанные на RSA сертификаты и требуются для продуктов, которые имеют сертификации Общих критериев (CC). Коммерческие решения правительства США для Классифицированных Систем (CSfC), программа требует сертификации CC и так, это включено в Выпуск 11.0 Cisco Unified Communications Manager и далее.

Сертификаты ECDSA доступны наряду с существующими сертификатами RSA в этих областях:

- Управление сертификатами

- Функция представительства сертифицирующей организации (CAPF)
- Отслеживание Transport Layer Security (TLS)
- Безопасные соединения SIP
- Менеджер интеграции компьютерной телефонии (CTI)
- HTTP и
- Энтропия

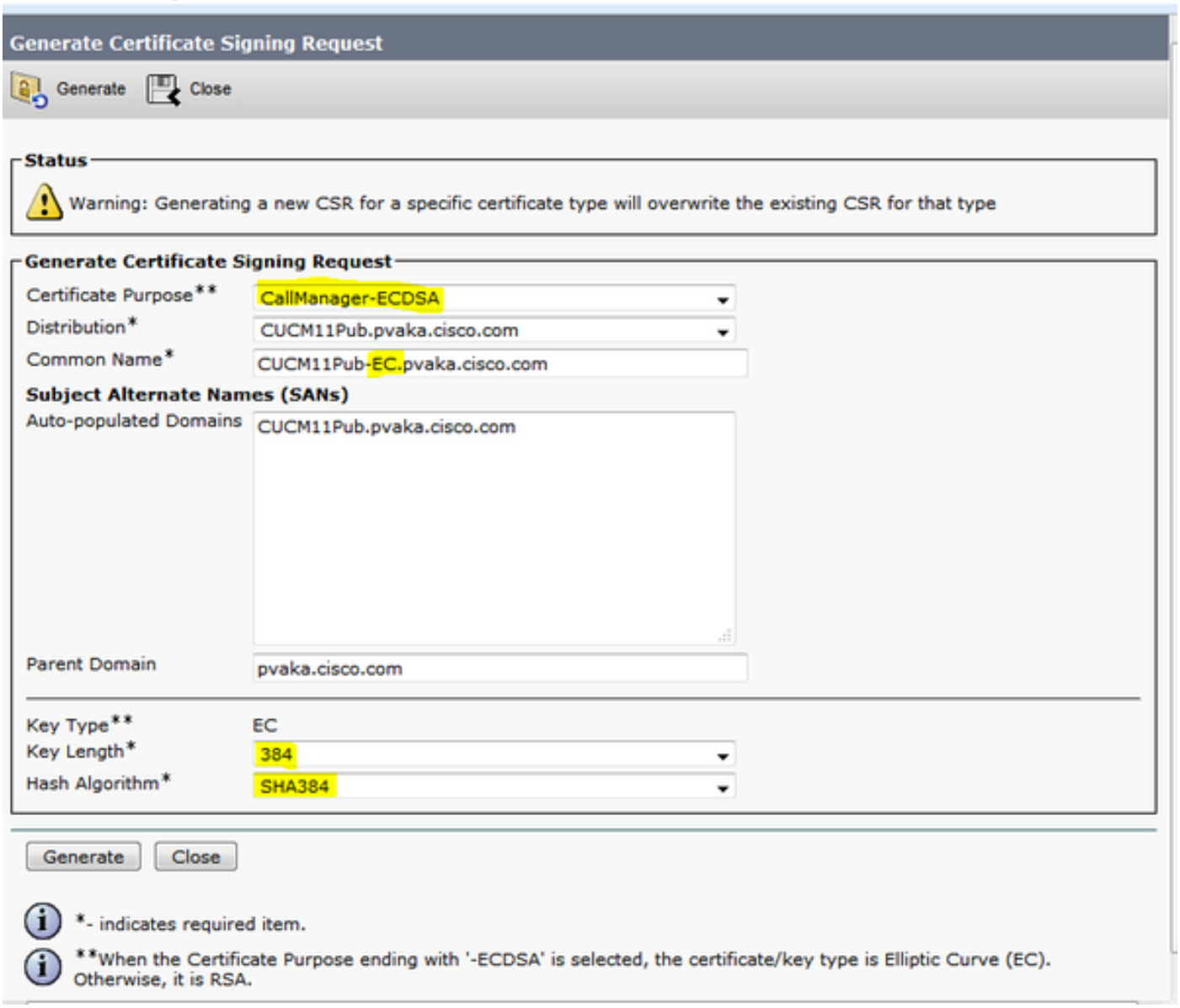
Следующие разделы предоставляют более подробную информацию о каждой из вышеупомянутых 7 областей.

Управление сертификатами

Генерация Сертификатов с шифрованием EC

Поддержка ECC от CUCM 11.0 и далее для генерации Сертификата CallManager с шифрованием EC

- Новая **опция CallManager-ECDSA**, доступная как показано в образе.
- Требует, чтобы часть, относящаяся к хосту общего имени закончилась в **- EC**, предотвратила наличие того же общего имени как сертификат **CallManager**.
- В случае Много сертификата SAN Сервера это должно закончиться в **- мс EC**.



- И запрос подписанного сертификата и запрос CSR ограничивают выборы алгоритма хэширования в зависимости от размера ключа EC.
- Для размера ключа EC 256 алгоритм хэширования может быть SHA256, SHA384 или SHA512. Для размера ключа EC 384 алгоритм хэширования может быть SHA384 или SHA512. Для размера ключа EC 521 единственная опция является SHA512.
- Размер ключа по умолчанию 384, и алгоритм хеширования по умолчанию является SHA384, который может быть изменен с помощью выпадающего. Доступные опции основываются на выбранном Размере ключа.

Конфигурация интерфейса командой строки CLI

Новый модуль сертификата назвал **CallManager-ECDSA**, был добавлен для команд CLI

- свидетельство набора regen [модуль] – восстанавливает подписанный сертификат

```
admin:set cert regen ?
Syntax:
set cert regen [name]
name mandatory unit name

admin:set cert regen CallManager-ECDSA

WARNING: This operation will overwrite any CA signed certificate previously imported for  CallManager-
ECDSA
Proceed with regeneration (yes|no)?
```

- свидетельство набора импортирует own|trust [модуль] – импорт CA подписанный сертификат

```
admin:set cert import trust CallManager-ECDSA
Paste the Certificate and Hit Enter
```

- набор csr генерал [модуль] – генерирует запрос подписи сертификата (CSR) для указанного **модуля**

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- объем набора export|consolidate|import tftp – Когда tftp является названием модуля, сертификаты CallManager-ECDSA, автовключен с сертификатами RSA CallManager в объемных операциях.

CTL и файлы ITL:

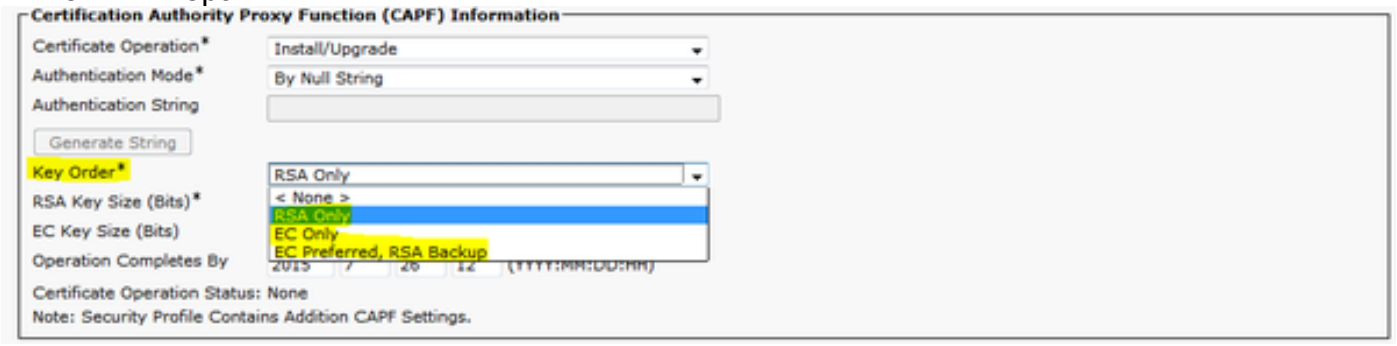
- И CTL и файлы ITL имеют подарок **CallManager-ECDSA**.
- Сертификат CallManager-ECDSA имеет Функцию CCM+TFTP и в ITL и в файле CTL.
- Можно использовать**, показывают ctl** или **команды show itl** для просмотра этой информации как показано в образе:

```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
6       SERIALNUMBER    16      61:E4:7E:DA:01:65:E4:68:22:9E:2E:CC:EB:35:18:DD
7       PUBLICKEY       270
8       SIGNATURE       256
9       CERTIFICATE     951     3B D9 E1 B0 68 56 5F ED 73 FF 75 B7 36 3B D1 29 9E 93 36 FD (SHA1 Hash HEX)

        ITL Record #:5
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1071
2       DNSNAME         26      CUCM11Pub.pvaka.cisco.com
3       SUBJECTNAME     68      CN=CUCM11Pub-EC.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      68      CN=CUCM11Pub-EC.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
6       SERIALNUMBER    16      60:28:0E:23:2C:DC:72:7D:16:B2:16:B1:40:90:20:7E
7       PUBLICKEY       97
8       SIGNATURE       104
9       CERTIFICATE     661     21 C4 B8 E9 71 B0 4C 90 C2 F9 93 30 E0 53 3D 1D DE 86 32 07 (SHA1 Hash HEX)

The ITL file was verified successfully.
```

- Можно использовать **utils ctl обновление** для генерации файла CTL.

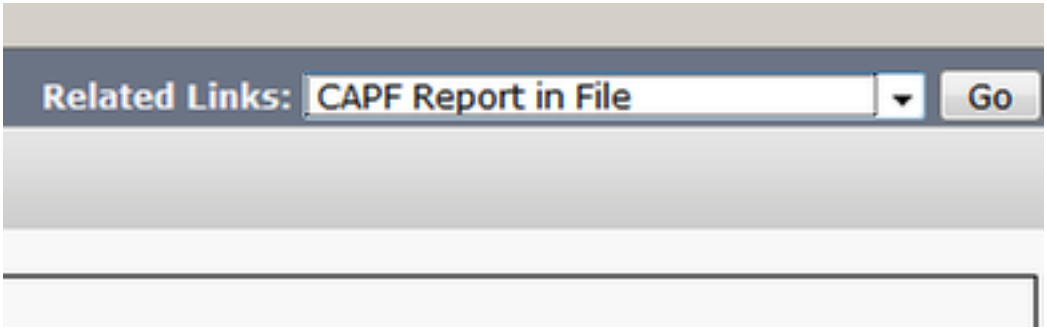
Функция представительства сертифицирующей организации (CAPF)

- Версия 3.0 CAPF в CUCM 11 оказывает поддержку для Размеров ключа EC наряду с RSA.
- Возможности Additional CAPF, предоставленные в дополнение к существующим полям CAPF, являются Ключевым Заказом и Размером ключа EC (биты).
- Существующий Размер ключа (биты) опция был изменен на Размер ключа RSA (биты).
- Ключевой Заказ оказывает поддержку для RSA Только, EC Только и Предпочтительное EC, опции резервной копии RSA.
- Размер ключа EC оказывает поддержку для Размеров ключа 256, 384 и 521 бит.
- Размер ключа RSA оказывает поддержку для 512, 1024 и 2048 битов
- Когда Ключевой Заказ RSA Только выбран, только Размер ключа RSA может быть выбран. Когда EC только выбрано, только Размер ключа EC может быть выбран. Когда Предпочтительное EC, резервная копия RSA выбрана, и RSA и Размер ключа EC могут быть выбраны.



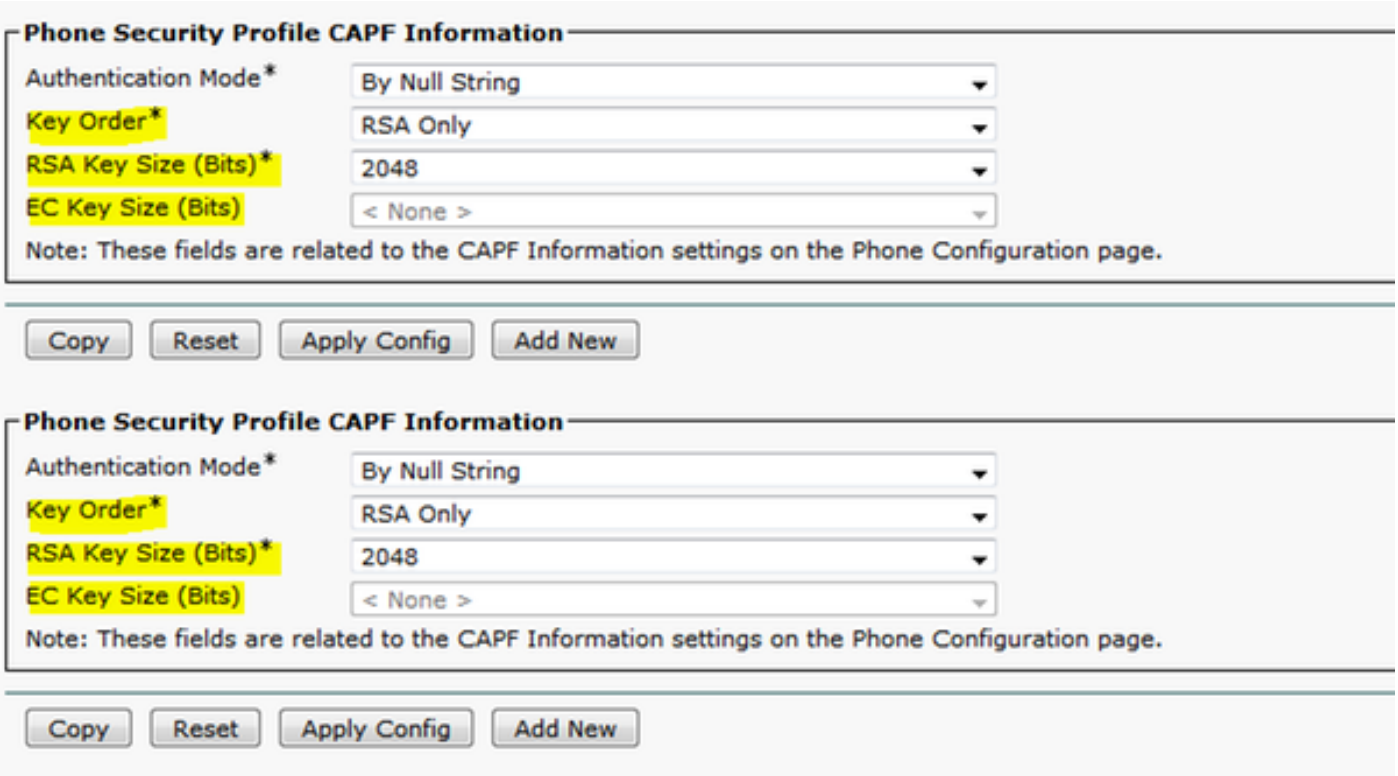
Дополнительные опции CAPF для телефона, телефонного профиля безопасности, конечного пользователя и страниц пользователя приложения

Device> Phone> Ссылки по теме



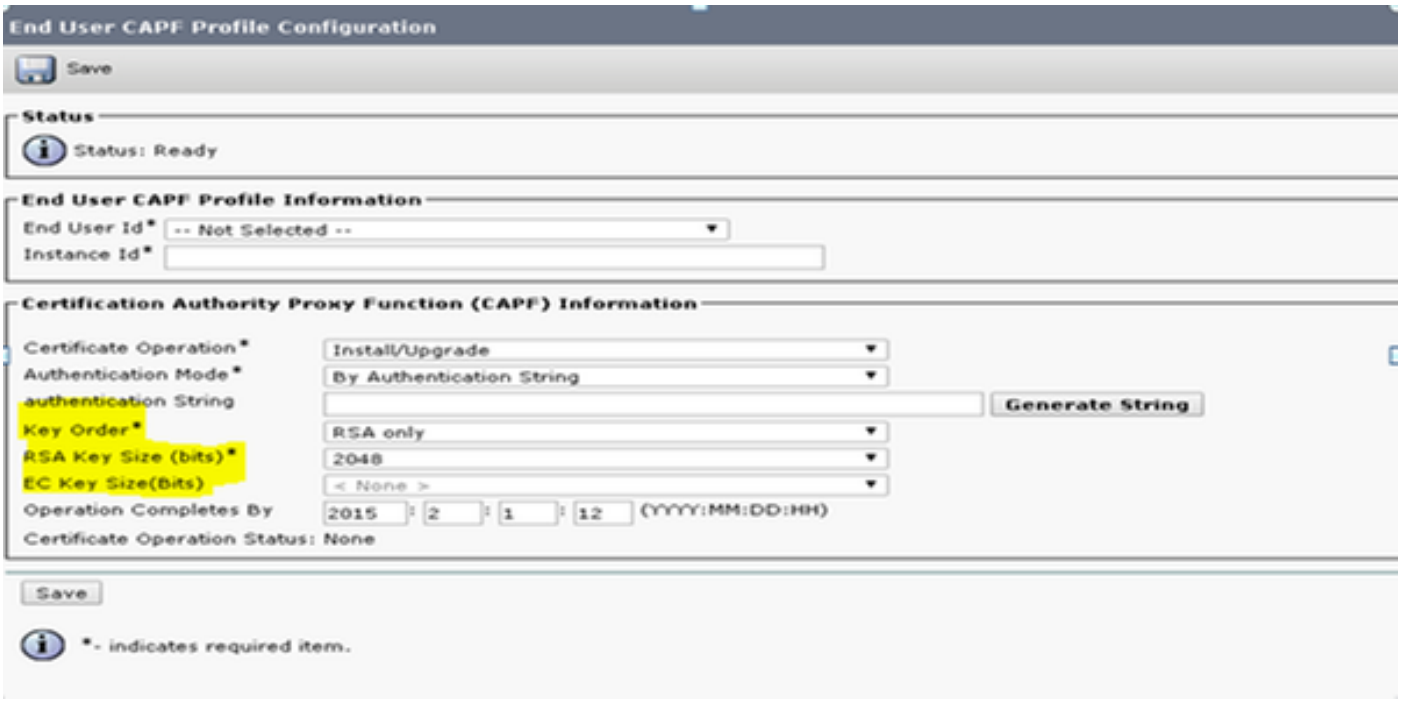
Перейдите к **Системному> Security> Телефонный профиль безопасности**

Управление пользователями> Параметры пользователя> Профиль CAPF Пользователя приложения



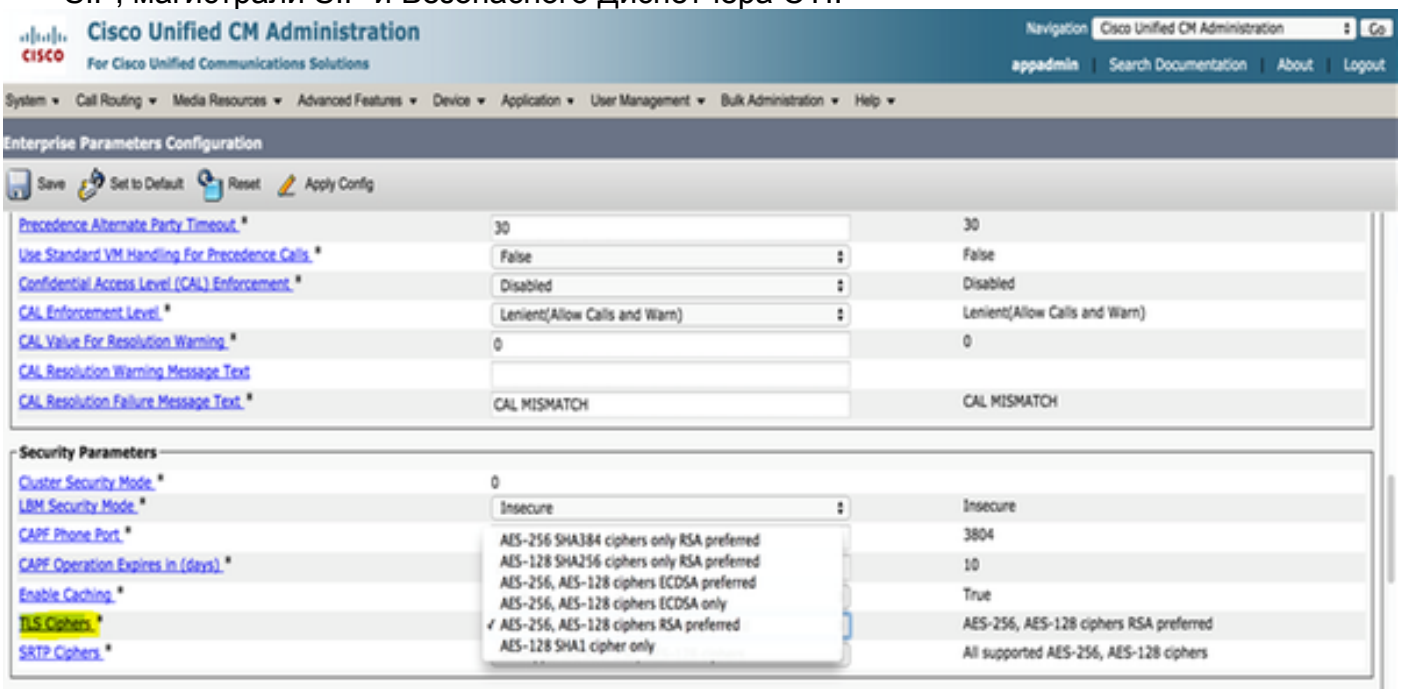
Navigaet к **Управлению пользователями> Параметры пользователя> Профиль CAPF**

Конечного пользователя.



Корпоративные параметры шифров TLS

- Шифры TLS Корпоративного параметра были обновлены для поддержки Шифров ECDSA.
- Шифры TLS Корпоративного параметра теперь устанавливают Шифры TLS для Линии SIP, магистрали SIP и Безопасного Диспетчера CTI.



SIP поддержка ECDSA

- Выпуск 11.0 Cisco Unified Communications Manager включает поддержку ECDSA линий SIP и интерфейсов магистрали SIP.
- Соединение между Cisco Unified Communications Manager и телефоном оконечной точки

или видеоустройством является соединением линии SIP, тогда как соединение между двумя Менеджерами Унифицированной связи Cisco является соединением магистрали SIP.
- Все соединения SIP поддерживают шифры ECDSA и используют сертификаты ECDSA.

Безопасный интерфейс SIP был обновлен для поддержки этих двух шифров

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Когда SIP делает (Transport Layer Security) TLS подключение, это сценарии:

- Когда SIP действует как сервер TLS

Когда интерфейс магистрали SIP действий Cisco Unified Communications Manager как сервер TLS для входящего безопасного соединения SIP, интерфейс магистрали SIP определяет, существует ли сертификат CallManager-ECDSA на диске. Если сертификат существует на диске, интерфейс магистрали SIP использует сертификат CallManager-ECDSA, если выбранный набор шифров

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 или
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- Когда SIP действует как клиент TLS

Когда действия интерфейса магистрали SIP как клиент TLS, интерфейс магистрали SIP передает список запрошенных наборов шифров к серверу на основе поля TLS Ciphers (который также включает опцию шифров ECDSA) в Корпоративных параметрах CUCM **Шифры TLS**. Эта конфигурация определяет список набора шифров клиента TLS и поддерживаемые наборы шифров в порядке предпочтения.

> **Примечание:** 1. Устройства, которые используют шифр ECDSA для создания соединения с CUCM, должны иметь сертификат CallManager-ECDSA в своем файле Идентификационного списка доверия (ITL).

> **Примечание:** 2. Интерфейс магистрали SIP поддерживает наборы шифров TLS RSA для соединений от клиентов, которые не поддерживают наборы шифров ECDSA или когда TLS подключение установлен с более ранней версией CUCM, которые не поддерживают ECDSA.

Защитите диспетчера CTI поддержка ECDSA

Безопасный интерфейс Диспетчера CTI был обновлен для поддержки этих четырех шифров:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

- Безопасный интерфейс Диспетчера CTI загружает и CallManager и сертификат CallManager-ECDSA. Это позволяет Безопасному интерфейсу Диспетчера CTI поддерживать новые шифры наряду с существующим шифром RSA.
- Подобный интерфейсу SIP, опция Enterprise Parameter TLS Ciphers в Cisco Unified Communications Manager используется для настройки шифров TLS, которые поддерживаются на Диспетчере CTI безопасный интерфейс.

Поддержка HTTPS загрузки конфигурации

- Для безопасной загрузки конфигурации (например, клиенты Jabber), Выпуск 11.0 Cisco Unified Communications Manager улучшен для поддержки HTTPS в дополнение к HTTP и интерфейсам TFTP, которые использовались в более ранних релизах.
- При необходимости обе обоюдных проверки подлинности использования клиента и сервера. Однако клиенты, которые зарегистрированы с LSC ECDSA и Зашифрованными конфигурациями TFTP, обязаны представлять свой LSC.
- Интерфейс HTTPS использует и CallManager и сертификаты CallManager-ECDSA как серверные сертификаты.

Примечание: 1. При обновлении CallManager, CallManager ECDSA или сертификаты Tomcat, необходимо деактивировать и повторно активировать Сервис TFTP.

Примечание: 2. Порт 6971 используется для аутентификации CallManager и сертификатов CallManager-ECDSA, используемых Телефонами.

Примечание: 3. Порт 6972 используется для аутентификации сертификатов Tomcat, используемых Jabber.

Энтропия

Энтропия является мерой случайности данных и помогает в определении минимального порога для общих требований критериев. Для имения строгого шифрования устойчивый источник энтропии требуется. Если алгоритм строгого шифрования, такой как ECDSA, использует слабый источник энтропии, шифрование может быть легко сломано.

В Выпуске 11.0 Cisco Unified Communications Manager улучшен энтропийный источник для Cisco Unified Communications Manager.

Демон Мониторинга энтропии является встроенной функцией, которая не требует конфигурации. Однако можно выключить его через CLI Cisco Unified Communications Manager.

Используйте следующие команды CLI для управления Энтропией, Контролирующей сервис Демона:

CLI Command	Description
utils service start Entropy Monitoring Daemon	Starts the Entropy Monitoring Daemon service.
utils service stop Entropy Monitoring Daemon	Stops the Entropy Monitoring Daemon service.
utils service active Entropy Monitoring Daemon	Activates the Entropy Monitoring Daemon service, which further loads the kernel module.
utils service deactive Entropy Monitoring Daemon	Deactivates the Entropy Monitoring Daemon service, which further unloads the kernel module.

Дополнительные сведения

- http://www. cisco . com/c/en/us/td/docs/voice_ip_comm/cucm/security/11_5_1/secugd/CUCM_BK_SEE2CFE1_00_cucm-security-guide-1151/CUCM_BK_SEE2CFE1_00_cucm-security-guide-1151_chapter_011.html#CUCM_RF_C0383C35_00l
- Cisco Systems – техническая поддержка и документация