Безопасный Cisco IP Phone под CUCM смешанный кластер режима

ID документа: 113333

Обновлено : 28 ноября 2011

Родственные продукты

- 7971G-GE унифицированного IP-телефона Cisco
- 7941G-GE унифицированного IP-телефона Cisco
- IP-телефон Cisco Unified 7970G
- IP-телефон Cisco Unified 7960G
- Унифицированный IP-телефон Cisco 7941G
- IP-телефон Cisco Unified 7961G
- + Покажите больше

Содержание

Введение

Этот документ описывает пошаговую процедуру для перемещения одного IP-телефона в безопасный режим от исходного кластера Cisco Unified Communication Manager (CUCM) до целевого кластера CUCM ни с кем вручную манипулирование файлом Сертифицированного трастового списка (CTL), установленным на таком IP-телефоне.

Примечание: Эта процедура независима от:

1. Протокол сигнализации используется телефоном. Предполагается, что протокол

сигнализации в источнике и кластере назначения остается тем же для определенного IP-телефона.
2. Модель телефона, которая исключает модели Cisco 7940/7960, потому что телефоны 7940/7960 требуют, чтобы вмешательство конечного пользователя ввело строку проверки подлинности, так как у них нет встроенного MIC.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, относятся к приложению Cisco Unified Communications Manager 7.x.

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.

Список надежных сертификатов

Все серверы в кластере CUCM генерируют подписанные сертификаты. Телефоны получают свои собственные сертификаты, который имеет два типа.

1. Производство установленного сертификата, данного Cisco, когда вы покупаете новый телефон.
2. Локально значительный сертификат вручен Функцией прокси полномочий Cisco.

CTL является списком подписанных сертификатов от всех серверов в кластере CUCM, которому может доверять телефон. CTL сохранен на сервере TFTP и передан IP-телефонам.

Устройство, файл и аутентификация сигнала полагаются на создание файла CTL, который создан, когда вы устанавливаете и настраиваете Клиента CTL Cisco на одиночной Рабочей станции Windows или сервере, который имеет USB-порт.

Файл CTL содержит серверный сертификат, открытый ключ, серийный номер, подпись, имя запрашивающей стороны, имя субъекта, функцию server, имя DNS и IP-адрес для каждого сервера. При настройке межсетевого экрана в файле CTL можно защитить Межсетевой экран Cisco ASA как часть безопасной системы Cisco Unified Communications Manager. Дисплеи клиента CTL Cisco сертификат межсетевого экрана как сертификат *CCM*. Администрирование Cisco Unified Communications Manager использует eToken для

аутентификации TLS подключение между Клиентом CTL Cisco и Поставщиком CTL Cisco.

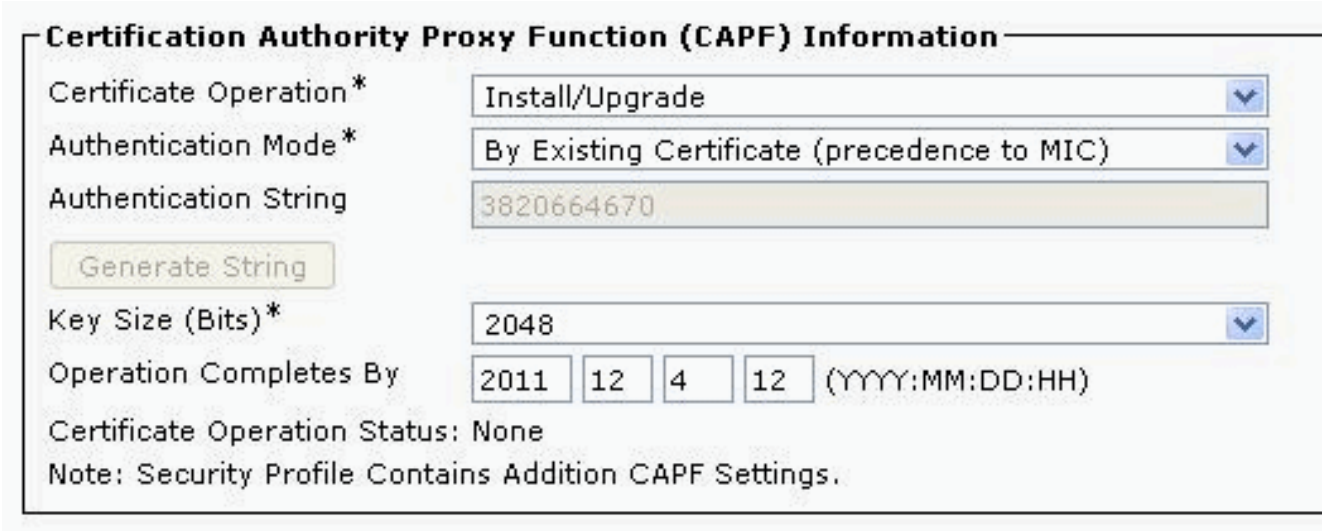
На версии 8. X CUCM и позже, IP-телефоны запрашивают файл CTL по умолчанию, даже если это не было создано. Файлы CTL не считают важными; они - просто часть новых характеристик безопасности, которые идут с CUCM 8. x. См. Настройку Клиент CTL Cisco для получения дополнительной информации.

Как защитить IP-телефон

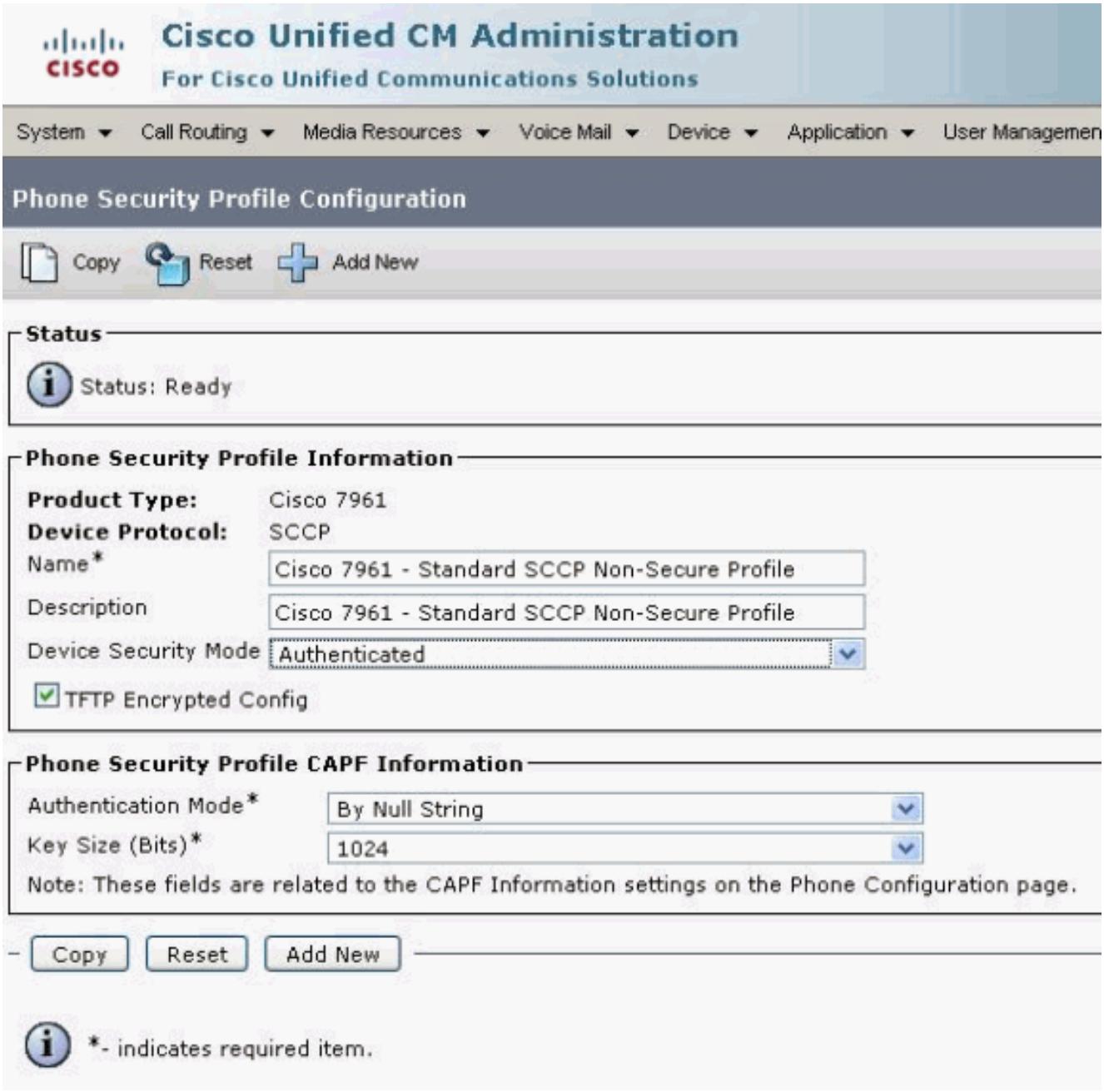
Для телефона для принятия файла CTL от любого кластера без потребности удалить существующую требует, чтобы файл CTL каждого кластера был подписан тем же совместно используемым набором eToken. Другими словами, мы должны создать Файл CTL для каждого кластера и подписать их всех с тем же eToken. Кроме того, чтобы к телефонам доверяют Централизованным серверам TFTP, также необходимо добавить Централизованные серверы TFTP в каждом Файле CTL.

Выполните эти шаги для настройки параметров безопасности для IP-телефона.

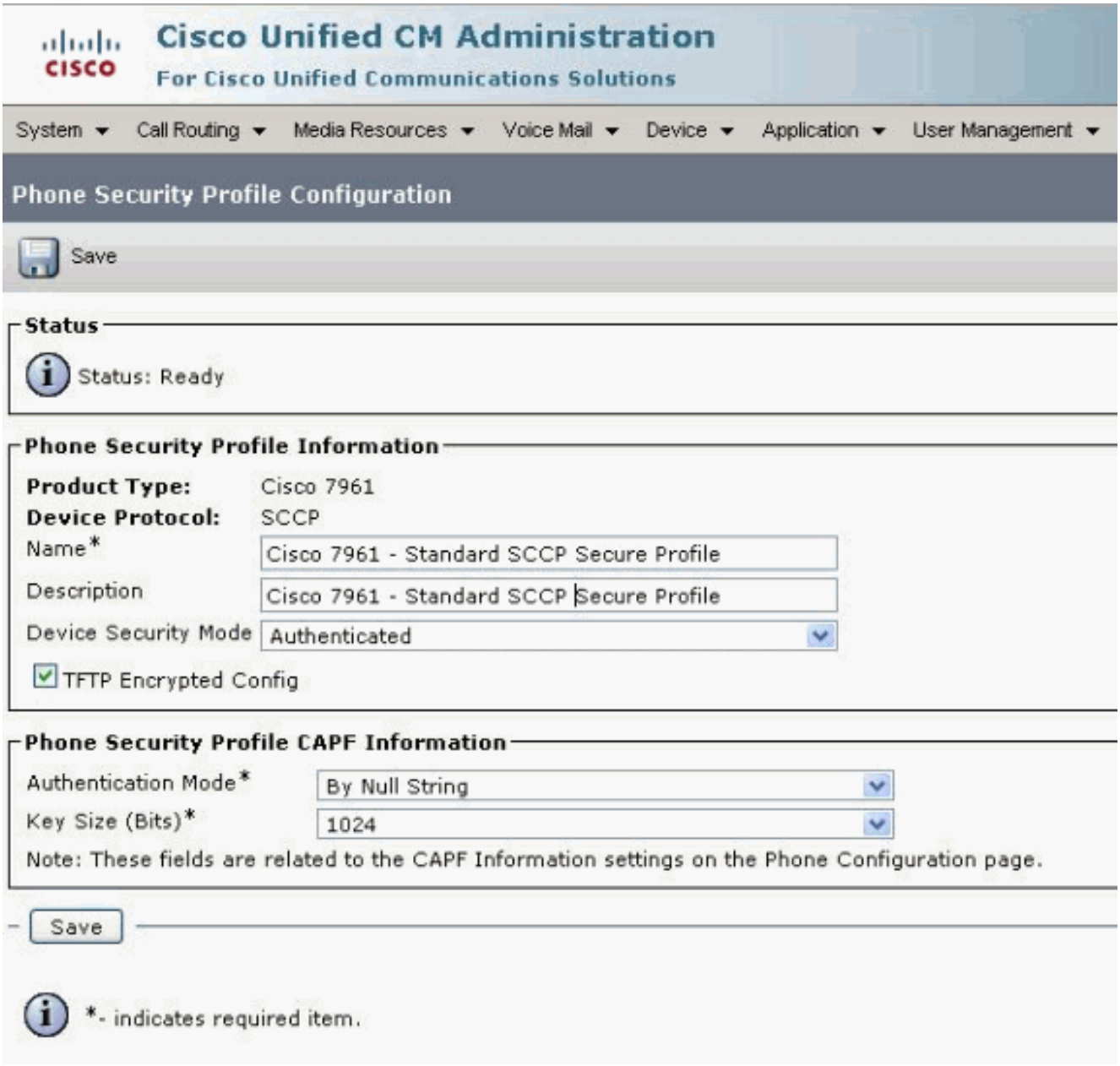
1. Настройте Профиль Безопасности устройства. Если надлежащая безопасность устройства Профиль не существует в выпадающем списке от страницы Настройки IP-телефона, оставляет его как по умолчанию, **Стандартный Незащищенный Профиль**.
2. Настройте информацию о Функции прокси центра сертификации (CAPF), для IP-телефона для получения нового LSC, подписанного целевым кластером CUCM.Это сделано на странице конфигурации телефона CUCM. Выберите значения из выпадающего меню как показано и затем нажмите **Save**.



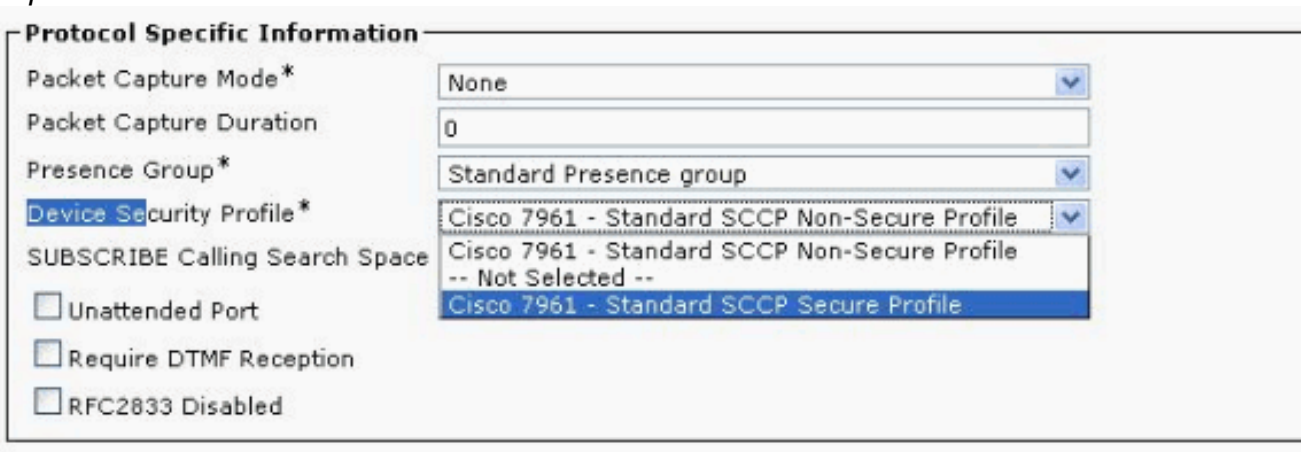
3. Настройте новый созданный Профиль Безопасности устройства:Выберите**> Security System Профиль> Телефонный Профиль безопасности**.**Нажмите кнопку "Найти".**Выберите тип телефона и введите подробные данные:



Нажмите **Copy**.Теперь **Сохраните** конфигурацию как показано здесь:



4. На странице Настройки IP-телефона, перепроверка, что настроен надлежащий *Режим безопасности устройства*.



5. Перезапустите IP-телефон.
6. Телефон должен теперь загрузить новый файл CTL от кластера назначения и должен подписать LSC от кластера назначения.
7. Телефон выполняется с Режимом безопасности, настроенным в Профиле Безопасности устройства.

Дополнительные сведения

- Рекомендация по вопросам безопасности: Переполнение кучи поставщика CTL Cisco Unified Communications Manager
- Безопасность IP-телефона и CTL (список надежных сертификатов)
- Поддержка голосовых технологий
- Поддержка продуктов Голосовой и Унифицированной связи
- Устранение неполадок в системах IP-телефонии Cisco
- Cisco Systems – техническая поддержка и документация

Соответствующие дискуссии сообщества технической поддержки Cisco

Сообщество технической поддержки Cisco является форумом, в котором можно задавать вопросы и получать ответы, обмениваться предложениями и сотрудничать со своими равноправными коллегами.

Обновлено : 28 ноября 2011
ID документа: 113333