Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Условные обозначения](#)
[Проблема - Неспособный применить процедуру использования подписанных сертификатов в руководстве.](#)
[Решение - Процедура для управления подписанными сертификатами для CVP 8.5](#)
[Дополнительные сведения](#)

Введение

Этот документ объясняет, как управлять подписанным сертификатом с подписанным сертификатом на файловой системе для Cisco Unified Customer Voice Portal (CVP) 8.5 (1) для управления .keystore содержимыми файла.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Cisco Унифицированный CVP 8.5.

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.

Проблема - Неспособный применить процедуру использования подписанных сертификатов в руководстве.

Задокументированная процедура замены подписанного сертификата с подписанным сертификатом на файловой системе больше не применяется:

Решение - Процедура для управления подписанными сертификатами для CVP 8.5

Для управления сертификатами в CVP 8.5 (1), необходимо управлять .keystore содержимыми файла.

Выполните следующие действия:

1. Откройте файл `%CVP_HOME%\conf\security.properties` для получения .keystore пароля. Необходимо будет перейти к `%CVP_HOME%` через целевой каталог установки для Унифицированного CVP (по умолчанию, это - C:\Cisco\CVP).
2. Файл свойств должен содержать одно свойство: Безопасность. keystorePW.
3. Для управления keystore после ввода команды keytool попросит вас вводить keystore пароль. Копируйте значение свойства Security.keystorePW и вставьте его в окно командной строки для ввода keystore пароля.Например, полагайте, что %CVP_HOME %\conf\security.properties файл содержит линию свойства:Паролем для копирования был бы `[3X}}E7@nhMXGy{ou.5AL!+4Ffm868`.
4. Создайте резервную копию %CVP_HOME %\conf\security каталог.
5. Откройте окно командной строки командной строки и изменитесь на каталог конфигурации безопасности:
6. Используйте запись с закрытым ключом для vxml_certificate, для создания запроса подписи сертификата, не забыв вводить keystore пароль, когда предложено. Новый csr файл будет создан на файловой системе:
7. Дайте файл запроса подписи сертификата (vxml_certificate.csr) доверенному центру сертификации. Они подпишутся, возвращая один или несколько надежных сертификатов.
8. Импортируйте файл подписанного сертификата (например, signed_vxml.crt) от вашего доверенного центра сертификации. Сертификаты должны быть импортированы в заказе цепочечной иерархии (root, промежуточное звено, подписанный сертификат).

Примечание: Это задокументировано в идентификатор ошибки Cisco CSCts21084 (только зарегистрированные клиенты).

Дополнительные сведения

- Руководства по конфигурации Cisco Unified Customer Voice Portal
- Cisco Systems – техническая поддержка и документация