Обновление сертификата на руководстве по конфигурации платформы Cisco Identity Services Engine

Содержание

Введение

Этот документ описывает оптимальные методы и упреждающие процедуры для возобновления сертификатов на платформе Cisco Identity Services Engine (ISE). Это также рассматривает, как установить сигналы тревоги и уведомления, таким образом, администраторы предупреждены относительно предстоящих событий, таких как окончание срока действия сертификата.

> **Примечание:** Этот документ не предназначен, чтобы быть руководством по поиску и устранению проблем для сертификатов.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Сертификаты X509
- Конфигурация Cisco ISE с сертификатами

Используемые компоненты

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

- Выпуск 1.2.0.899 Cisco ISE
- Устройство или VMware

Общие сведения

Как администратор ISE, вы в конечном счете встретитесь с фактом, что истекают сертификаты ISE. Если ваш сервер ISE имеет просроченный сертификат, серьезные проблемы могли бы возникнуть, пока вы не заменяете просроченный сертификат новым, подтвержденным сертификатом.

> **Примечание:** Если сертификат, который используется для Протокола EAP, истекает, все аутентификации могли бы отказать, потому что клиенты больше не доверяют сертификату ISE. Если сертификат протокола HTTPS истекает, риск еще больше: администратор не мог бы быть в состоянии войти к ISE больше, и распределенное развертывание могло бы прекратить функционировать и реплицировать.

В данном примере ISE имеет установленный сертификат от сервера Центра сертификации (CA), который истечет через один месяц. Администратор ISE должен установить новое, подтвержденный сертификат на ISE, прежде чем истечет старый сертификат. Этот упреждающий подход предотвращает или минимизирует время простоя и избегает влияния на ваших конечных пользователей. Как только период времени нового установленного сертификата начинается, можно включить EAP и/или протокол HTTPS на новом сертификате.

Можно настроить ISE так, чтобы он генерировал сигналы тревоги и уведомил администратора для установки новых сертификатов, прежде чем истекут старые сертификаты.

> **Примечание:** Этот документ использует HTTPS с подписанным сертификатом для демонстрации влияния обновления сертификата, но этот подход не рекомендуется для оперативной системы. Лучше использовать сертификат CA и для EAP и для протоколов HTTPS.

Настройка

Обзорные подписанные сертификаты ISE

Когда ISE установлен, он генерирует подписанный сертификат. Подписанный сертификат используется для административного доступа и для связи в рамках распределенного развертывания (HTTPS), а также для проверки подлинности пользователя (EAP). В оперативной системе используйте сертификат CA вместо подписанного сертификата.

> **Совет:** См. Управление сертификатами в разделе Cisco ISE Руководства по установке оборудования платформы Cisco Identity Services Engine, Выпуска 1.2 для дополнительных сведений.

Форматом для сертификата ISE должен быть Privacy Enhanced Mail (PEM) или Выдающиеся правила кодирования (DER).

Для просмотра начального подписанного сертификата перейдите к **администрированию> Система> Сертификаты> Локальные Сертификаты** в консоли ISE:

Если вы устанавливаете серверный сертификат на ISE через Запрос подписи сертификата (CSR) и изменяете сертификат для HTTPS или протокола EAP, самоподписанный серверный сертификат все еще присутствует, но больше не используется.

> **Внимание. :** Для изменений протокола HTTPS требуется перезапуск сервисов ISE, который создает несколько минут времени простоя. Изменения протокола EAP не инициируют перезапуск сервисов ISE и не вызывают время простоя.

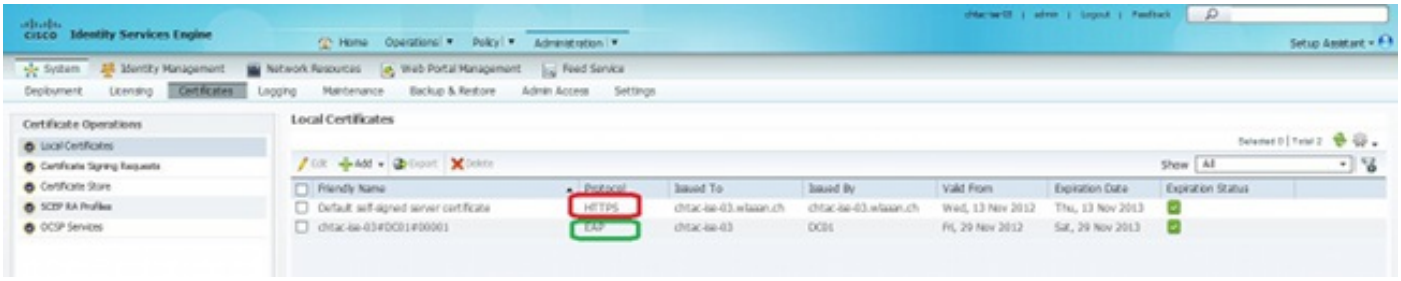
Определите, когда изменить сертификат

Предположите, что установленный сертификат скоро истекает. Лучше позволить сертификату истечь перед возобновлением его или изменить сертификат перед истечением? Необходимо изменить сертификат перед истечением так, чтобы у вас было время, чтобы запланировать подкачку сертификата и управлять любым временем простоя, вызванным подкачкой.

Когда необходимо изменить сертификат? Получите новый сертификат с датой начала, которая предшествует дате окончания действия старого сертификата. Период времени между теми двумя датами является окном изменения.

> **Внимание. :** При включении HTTPS он вызывает сервисный перезапуск на сервере ISE, и вы испытываете несколько минут времени простоя.

Этот образ изображает информацию для сертификата, который выполнен CA и истекает 29 ноября 2013:



Генерируйте запрос подписи сертификата

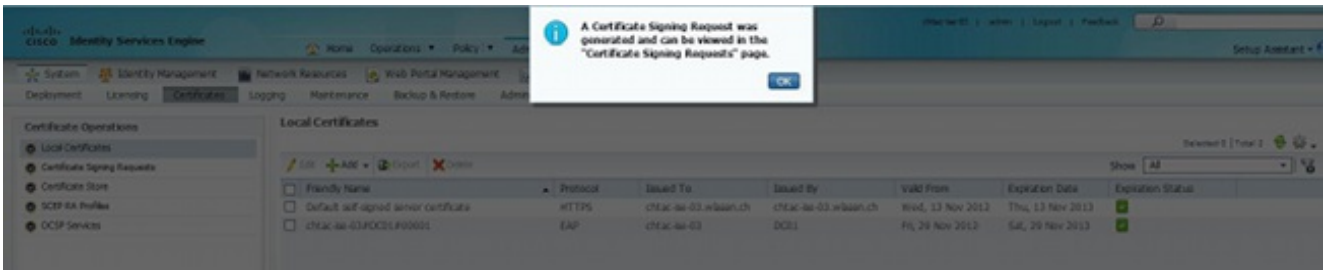
Эта процедура описывает, как возобновить сертификат через CSR:

1. В консоли ISE перейдите для **Добавления>, Генерируют Запрос подписи сертификата**.

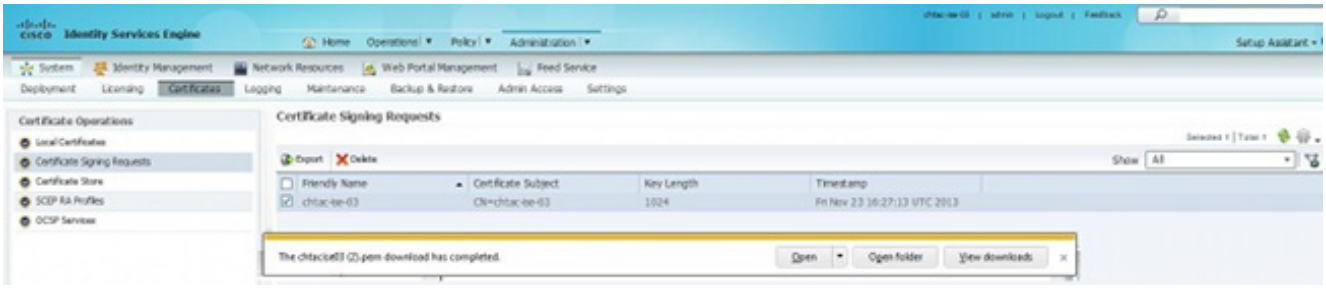
2. Минимальной информацией, которую необходимо ввести в текстовое поле **Предмета Сертификата**, является *CN=ISEfqdn*, где *ISEfqdn* является Полное доменное имя (FQDN) ISE. Добавьте дополнительные поля, такие как O (Организация), OU (Подразделение) или (страна) К в Предмете Сертификата с использованием запятых:

3. Одна из линий текстового поля **альтернативного имени субъекта (SAN)** должна повторить ISE FQDN. Если вы хотите использовать альтернативные названия или сертификат подстановочного знака, можно добавить второе поле SAN.

4. Всплывающее окно указывает, завершены ли поля CSR правильно:



5. Для экспортирования CSR нажмите **Certificate Signing Requests** в левой панели, выберите CSR и нажмите **Export**:

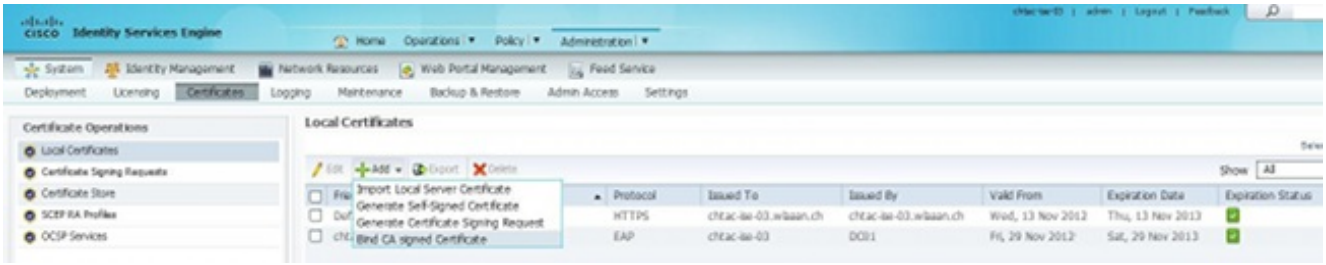


6. CSR сохранен на вашем компьютере. Отправьте его своему CA для подписи.

Установите сертификат

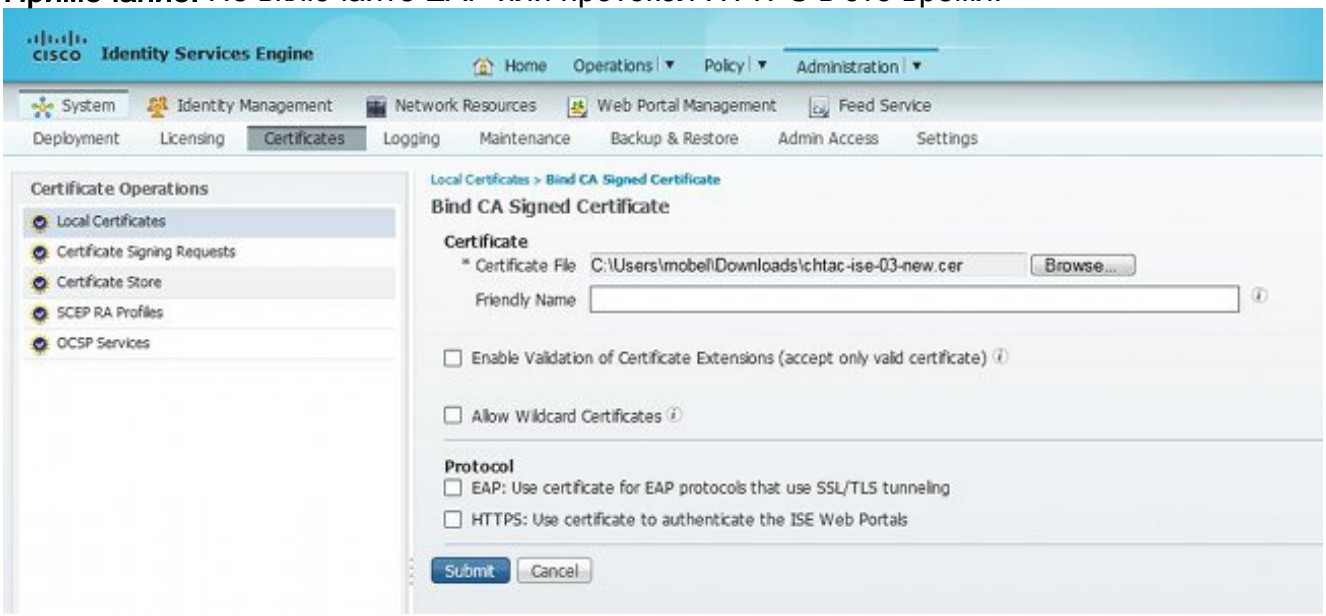
Как только вы получаете заключительный сертификат от своего CA, необходимо добавить сертификат к ISE:

1. В консоли ISE нажмите **Local Certificates** в левой панели, затем **нажмите Add** и **Свяжите подписанный сертификат CA**:

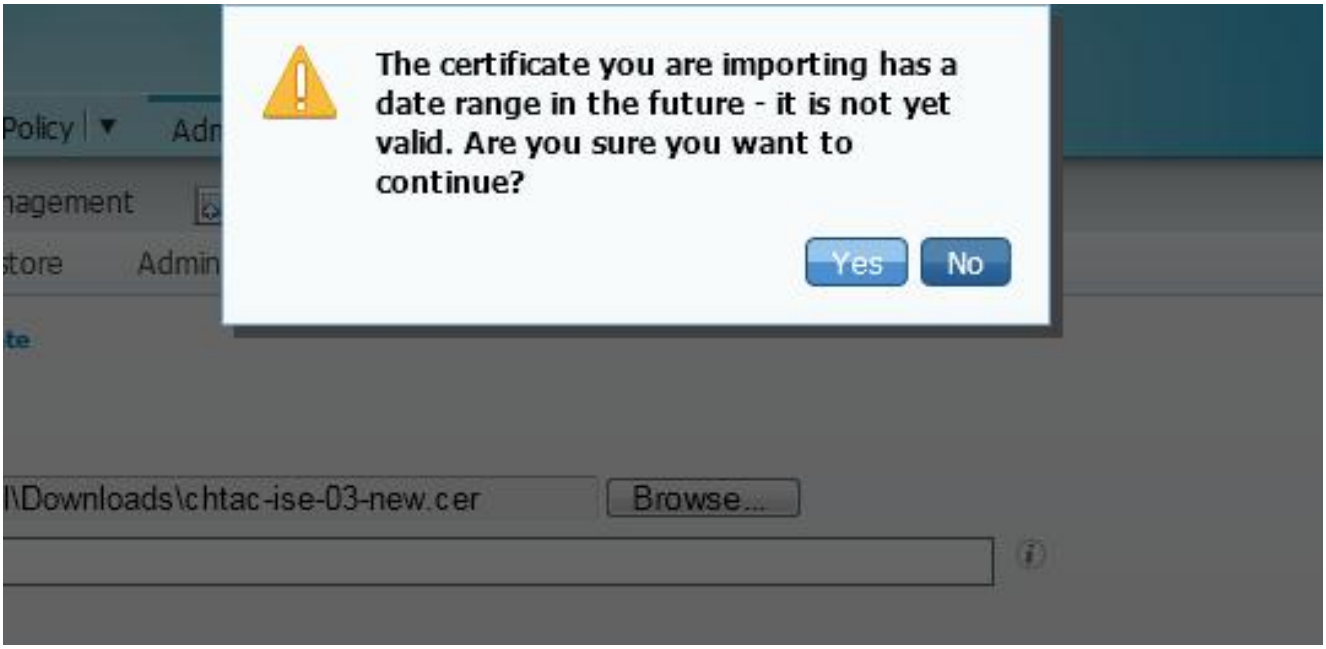


2. Введите простое, ясное описание сертификата в **Дружественном** текстовом поле **Названия**:

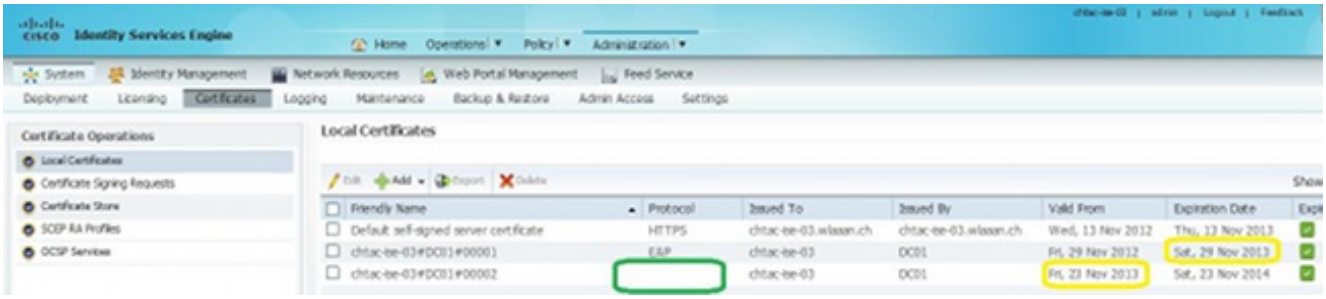
   Примечание: Не включайте EAP или протокол HTTPS в это время.



3. Поскольку вы устанавливаете новый сертификат, прежде чем старый истечет, вы видите ошибку, которая сообщает о диапазоне дат в будущем (23 ноября 2013 в данном примере).



4. Нажмите **Yes** для продолжения. Сертификат теперь установлен, но не в использовании, как выделено в зеленом. Наложение между датой окончания действия и допустимой датой выделено в желтом цвете:



Примечание: При использовании подписанных сертификатов в распределенном развертывании основной подписанный сертификат должен быть установлен в хранилище надежного сертификата вторичного сервера ISE. Аналогично, вторичный подписанный сертификат должен быть установлен в хранилище надежного сертификата основного сервера ISE. Это позволяет серверам ISE взаимно аутентифицировать друг друга. Без этого могли бы сломаться развертывания. Если вы возобновляете сертификаты от независимого поставщика CA, проверяете, изменила ли цепочка корневого сертификата и обновляет хранилище надежного сертификата в ISE соответственно. И в сценариях, гарантируйте, что узлы ISE, операционные системы оконечной точки и соискатели в состоянии проверить цепочку корневого сертификата.

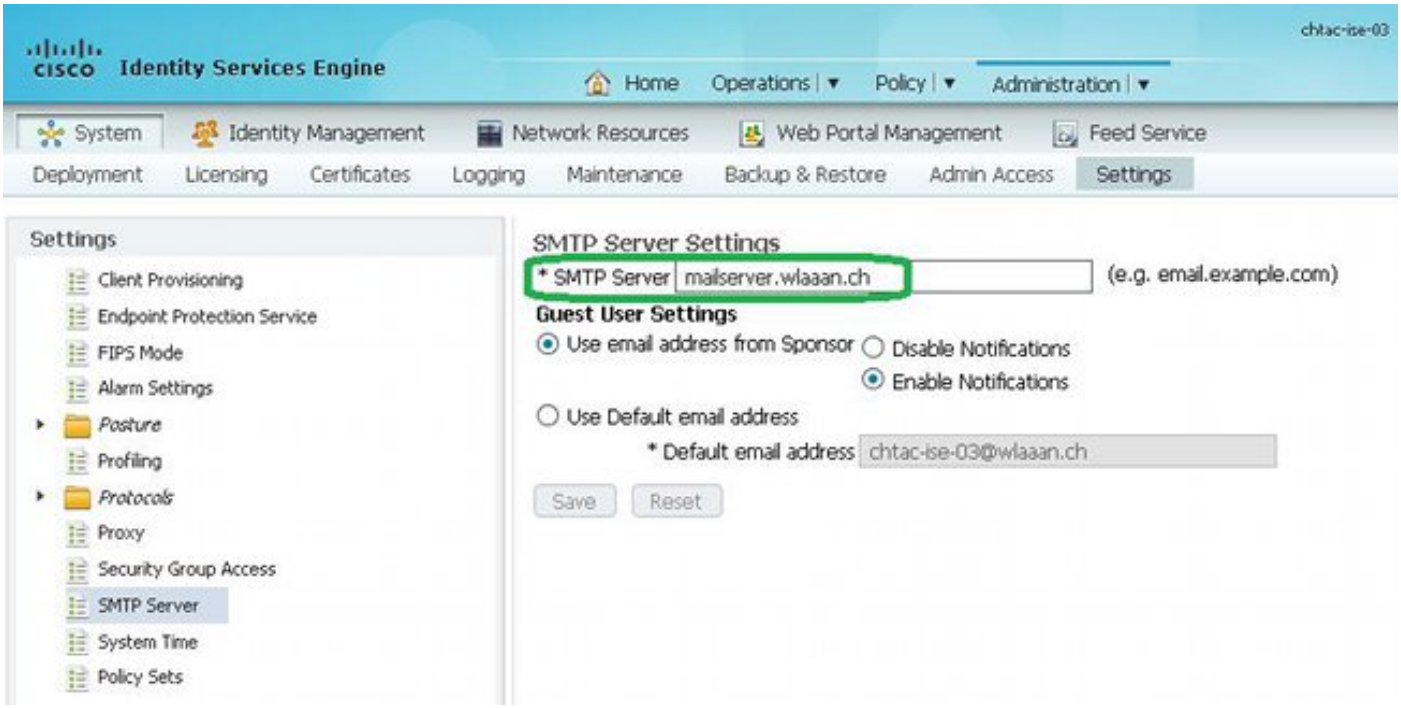
Настройте систему предупреждения

Когда дата окончания действия локального сертификата в течение 90 дней, Cisco ISE уведомляет вас. Такое предварительное уведомление помогает вам избегать просроченных сертификатов, планировать изменение сертификата, и предотвращать или минимизировать время простоя.

Уведомление появляется несколькими способами:

- Цветные значки состояния истечения появляются на странице Local Certificates.
- Сообщения об окончании срока действия появляются в отчёте о Системной диагностике Cisco ISE.
- Сигналы тревоги истечения генерируются в 90 дней и 60 дней, затем ежедневно за заключительные 30 дней перед истечением.

Настройте ISE для почтового уведомления сигналов тревоги истечения. В консоли ISE перейдите к **администрированию> Система> Параметры настройки> Сервер SMTP**, определите сервер Протокола SMTP и определите другие настройки сервера так, чтобы почтовые уведомления были переданы за сигналами тревоги:

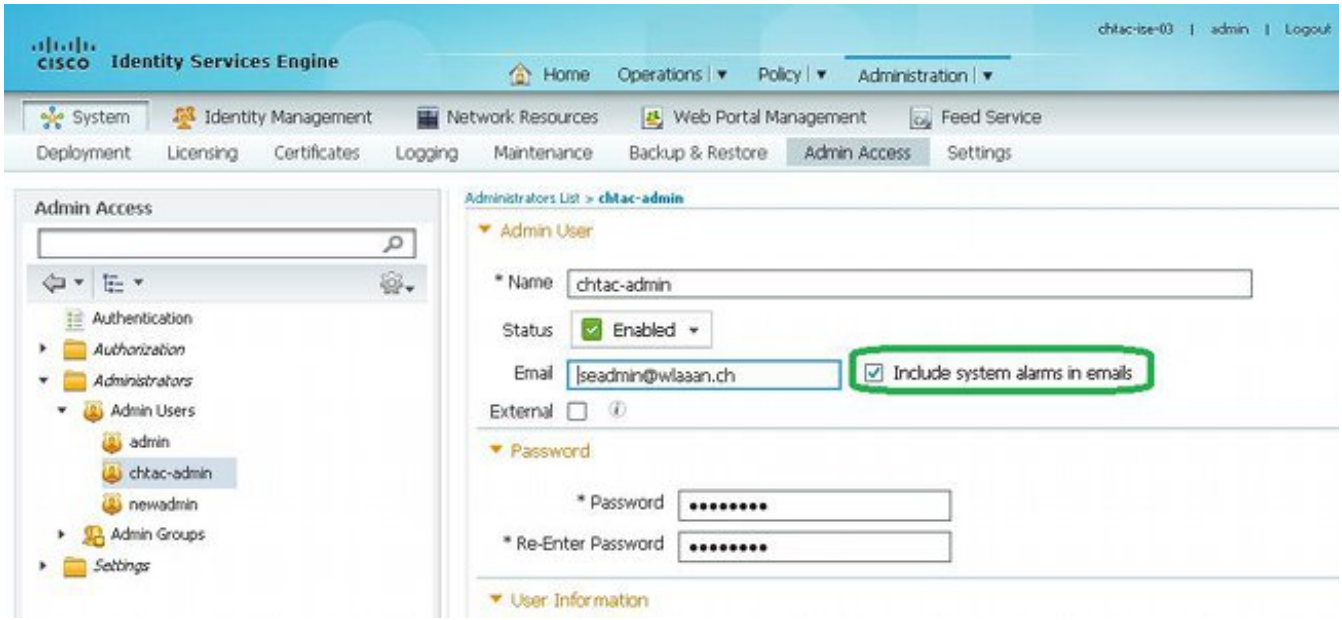


Существует два способа, которыми можно установить уведомления:

- Используйте Доступ администратора для уведомления администраторов:

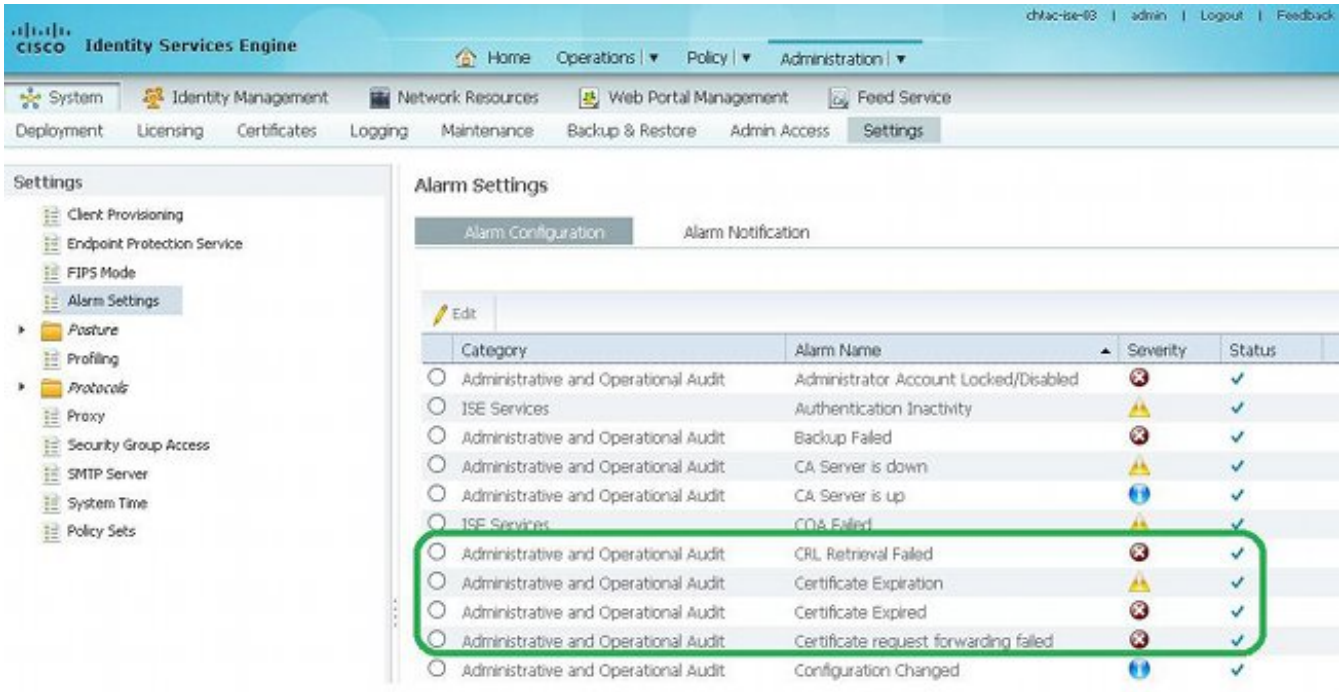
  Перейдите к **администрированию> Система> Доступ администратора> Администраторы> пользователи Admin**.

  Проверьте **Включать системные сигналы во** флажке **электронных почт** для пользователей Admin, которые должны получить аварийные оповещения. Адрес электронной почты для отправителя аварийных оповещений жестко закодирован как *ise@hostname*.

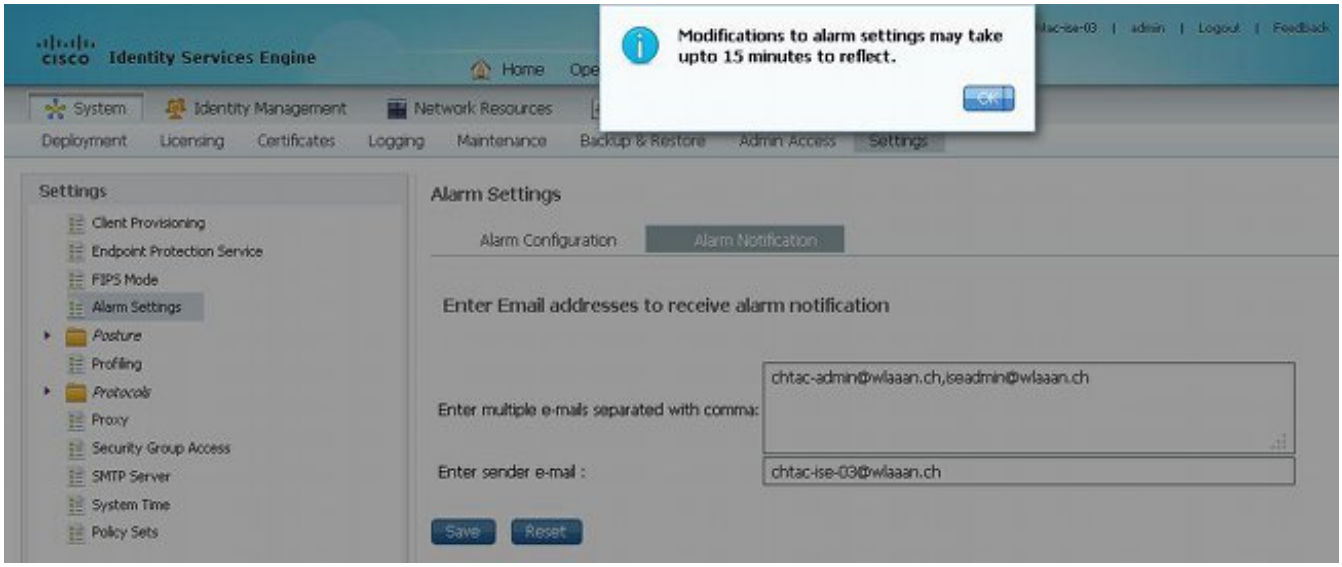


- Настройте настройки аварийных сигналов ISE для уведомления пользователей:

  Перейдите к **администрированию> Система> Параметры настройки> Настройки аварийных сигналов> Конфигурация аварийных сигналов**:



Примечание: Отключите Статус для категории, если вы хотите предотвратить сигналы тревоги от той категории.Нажмите **Alarm Notification,** введите адреса электронной почты пользователей, чтобы быть уведомленными и сохраните изменение конфигурации. Изменения могли бы взять за 15 минут до того, как они будут активны.

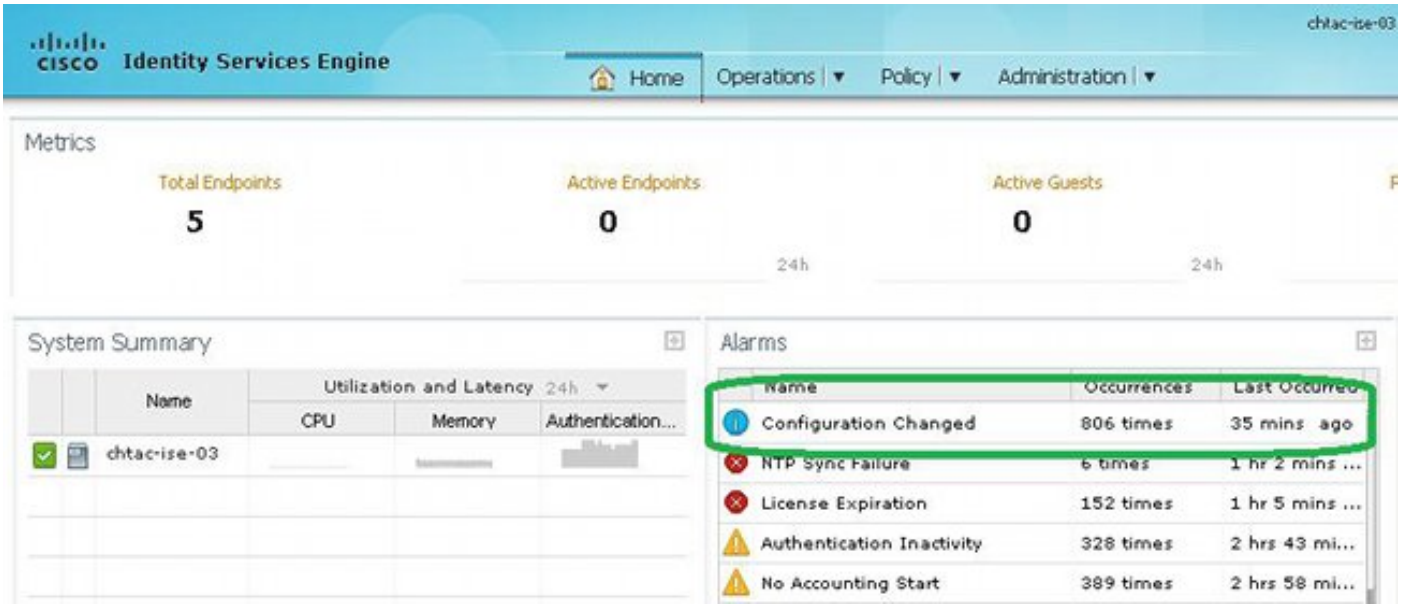


Проверка

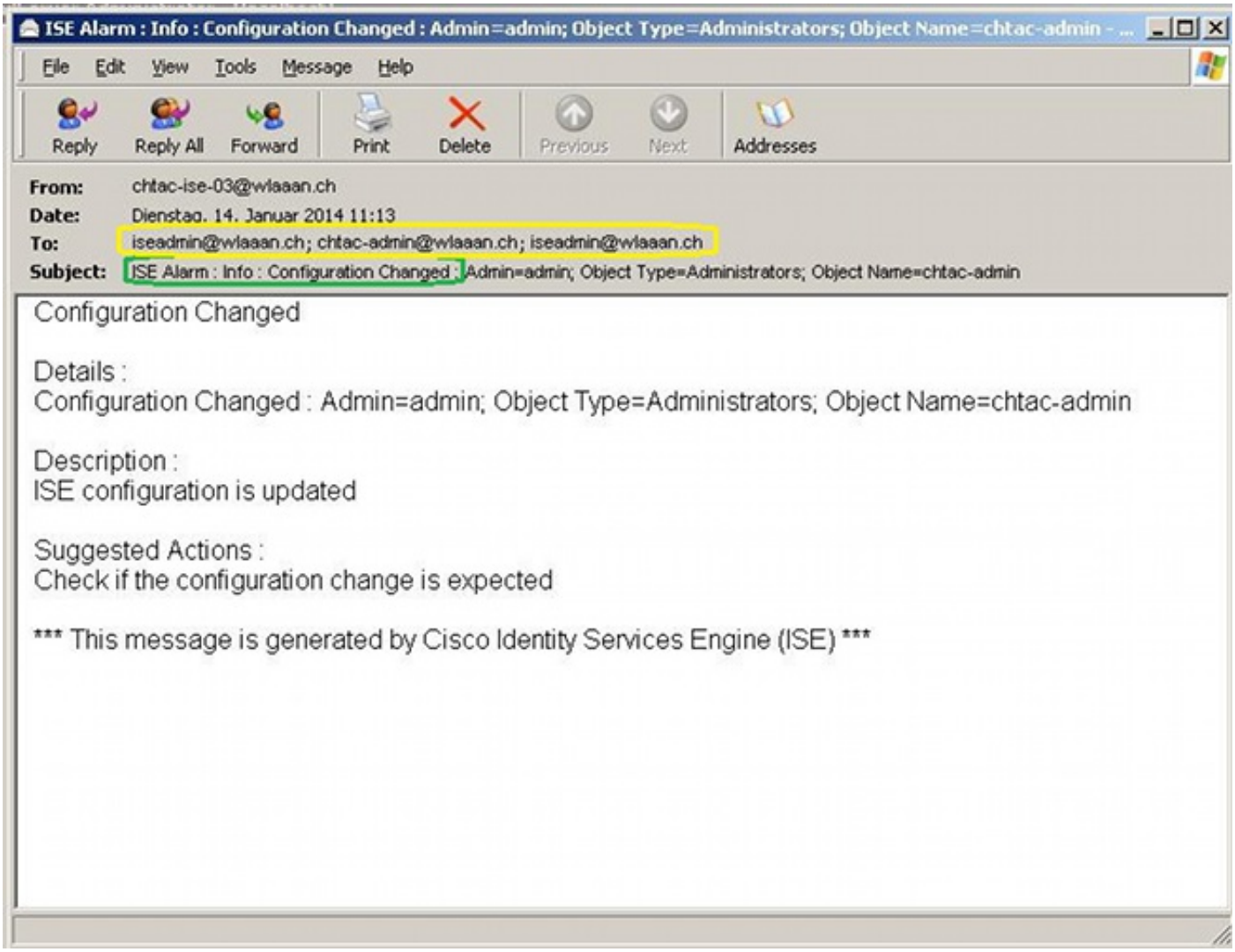
Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Проверьте систему предупреждения

Проверьте, что система предупреждения работает правильно. В данном примере изменение конфигурации генерирует предупреждение с уровнем важности информации. (Информационный аварийный сигнал является самыми низкими степенями серьезности ошибки, в то время как окончания срока действия сертификата генерируют уровень более высокого уровня важности Предупреждения.)



Это - пример почтового сигнала тревоги, который передается ISE:



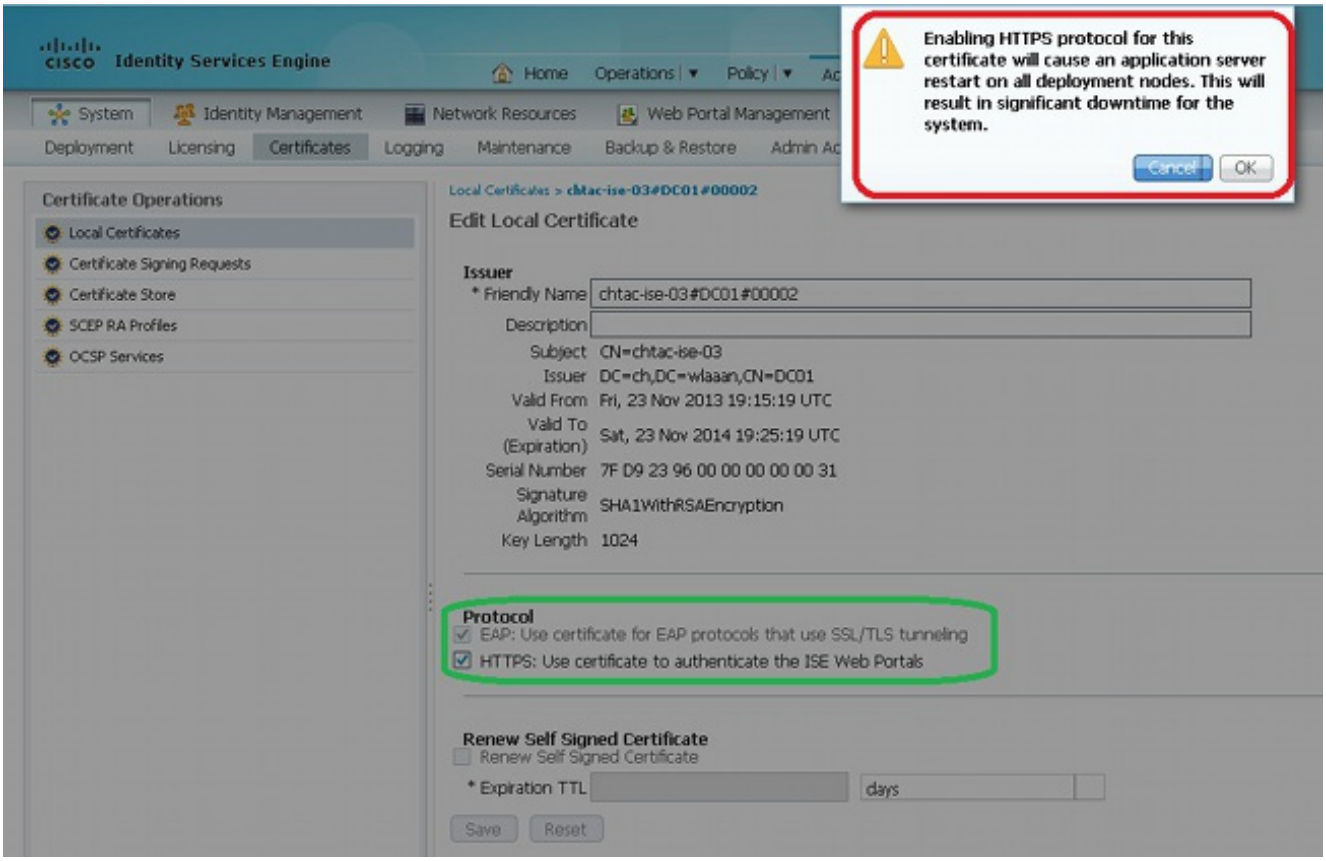
Примечание: В данном примере ISE передает почтовое аварийное сообщение дважды к iseadmin@wlaaan.ch, как выделено в желтом цвете. Этот адрес электронной почты был установлен для получения уведомлений обоими методами, объясненными в, Настраивают Систему предупреждения.

Проверьте изменение сертификата

Эта процедура описывает, как проверить, что сертификат установлен правильно и как изменить протоколы для EAP и/или HTTPS:

1. На консоли ISE перейдите к **администрированию> Сертификаты> Локальные Сертификаты** и выберите новый сертификат, чтобы посмотреть детали.

   Внимание. : Если вы включаете протокол HTTPS, перезапуски сервиса ISE, который вызывает простой сервера.



В данном примере предположите, что HTTPS перезапускает сервис ISE.

2. Для проверки статуса сертификата на сервере ISE введите эту команду в CLI:

```
CLI:> show application status ise
```

3. Как только все сервисы активны, пытаются войти как администратор.

4. Для сценария распределенного развертывания перейдите к **администрированию> Система> Развертывания> Состояние узла** на консоли ISE и проверьте состояние узла.

5. Проверьте, что аутентификация конечного пользователя успешна. На консоли ISE перейдите к **Операциям> Аутентификации** и рассмотрите сертификат для Защищенного расширяемого протокола аутентификации (PEAP)/EAP-Transport Безопасность Уровня (TLS) аутентификация.

Проверьте сертификат

Если вы хотите проверить сертификат внешне, можно использовать встроенные программные средства Microsoft Windows или инструментарий OpenSSL.

OpenSSL является реализацией с открытым исходным кодом протокола Уровня защищенных сокетов (SSL). Если сертификаты используют ваш собственный частный CA, необходимо разместить корневой сертификат CA в локальный компьютер и использовать опцию OpenSSL-*CApath*. Если у вас есть промежуточное звено CA, необходимо разместить его в тот же каталог также.

Чтобы получить общую информацию о сертификате и проверить его, используйте:

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

Могло бы также быть полезно преобразовать сертификаты с инструментарием OpenSSL:

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Заключение

Поскольку можно установить новый сертификат на ISE, прежде чем это будет активно, Cisco рекомендует установить новый сертификат, прежде чем истечет старый сертификат. Этот период наложения между старой датой окончания срока действия сертификата и новой датой начала сертификата дает вам время, чтобы возобновить сертификаты и запланировать их установку с минимальным временем простоя. Как только новый сертификат вводит свой допустимый диапазон дат, включите протокол HTTPS и/или EAP. Помните при включении HTTPS будет сервисный перезапуск.