Настройте доступ HTTPS для диагностического программного средства портика платформы UCCE с подписанным сертификатом центра сертификации (CA)

Содержание

Введение

Этот документ описывает процесс конфигурирования о том, как установить подписанный сертификат CA для программного средства Портика Платформы Диагностики Унифицированного предприятия Contact Center (UCCE).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Active Directory
- Сервер Системы доменных имен (DNS)
- CA инфраструктура развернулась и работающий для всех серверов и клиента
- Диагностический портик платформы

Доступ к Диагностическому программному средству Портика Платформы путем ввода IP-адреса в браузере, не получая сертификат, предупреждающий, вне области этой статьи.

Используемые компоненты

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

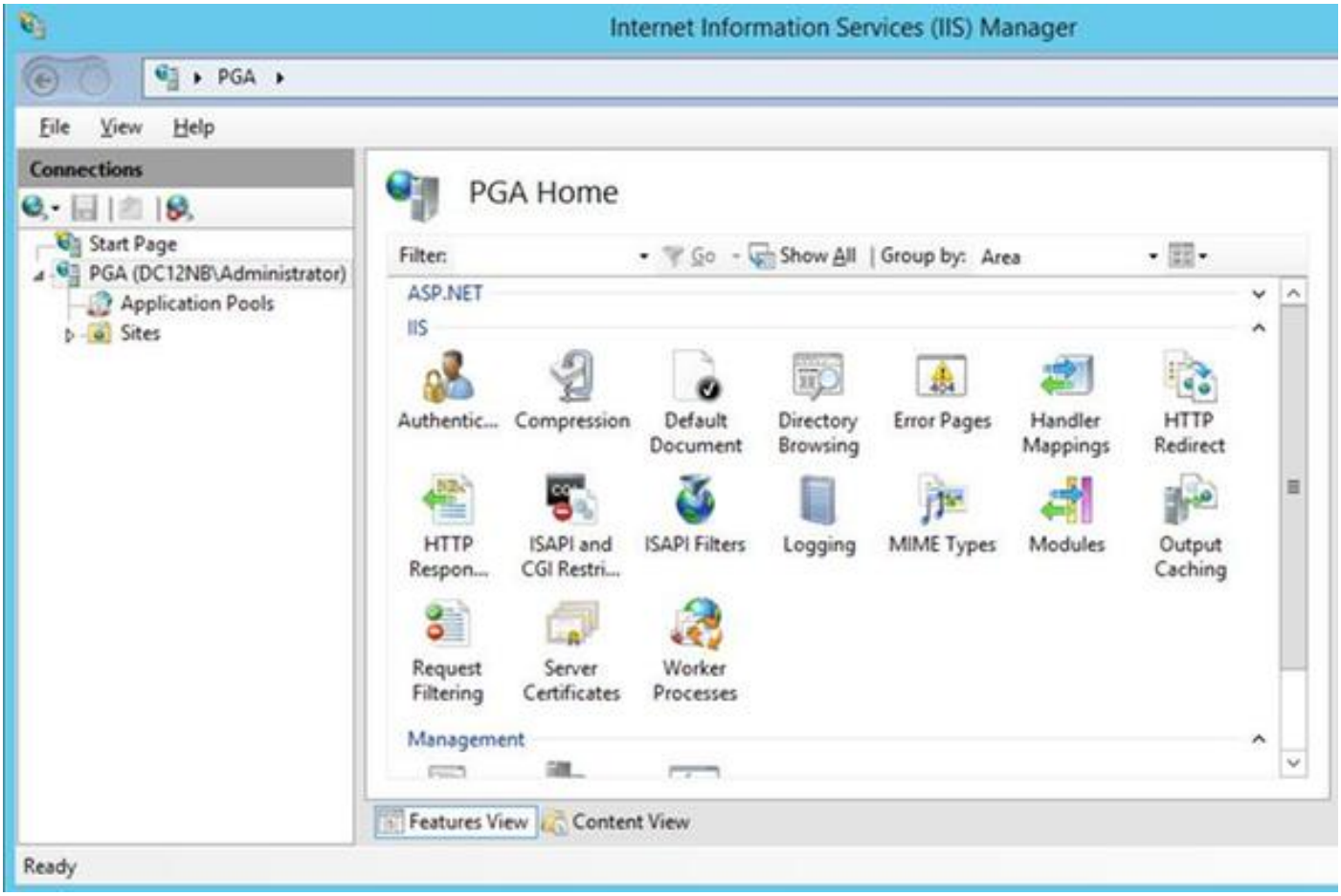
- Cisco UCCE 11.0.1
- Microsoft Windows server 2012 R2
- Центр сертификации R2 Microsoft Windows server 2012 года
- Microsoft Windows 7 SP1 ОС

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.

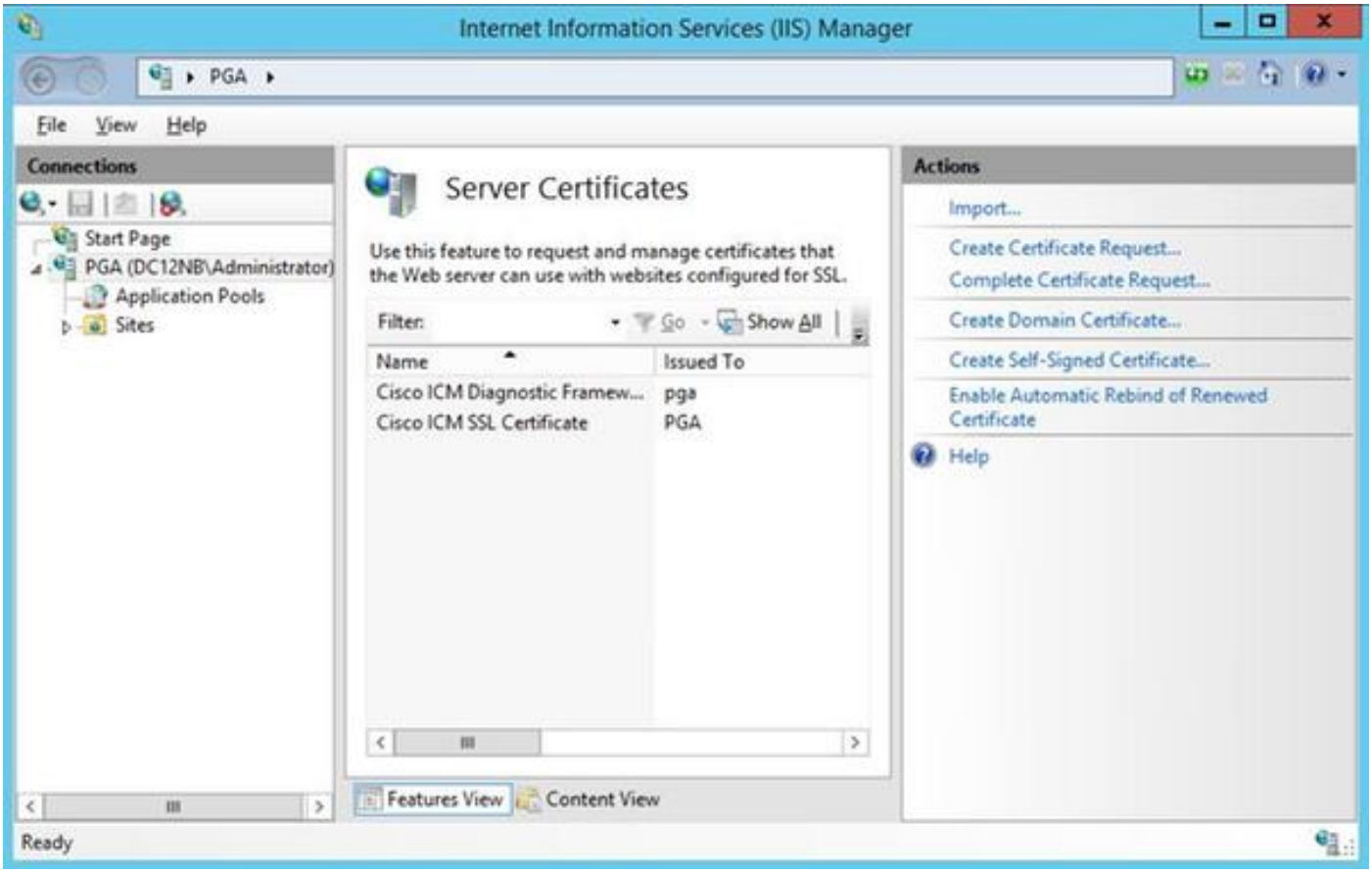
Настройка

Генерируйте сертификат запрос со знаком

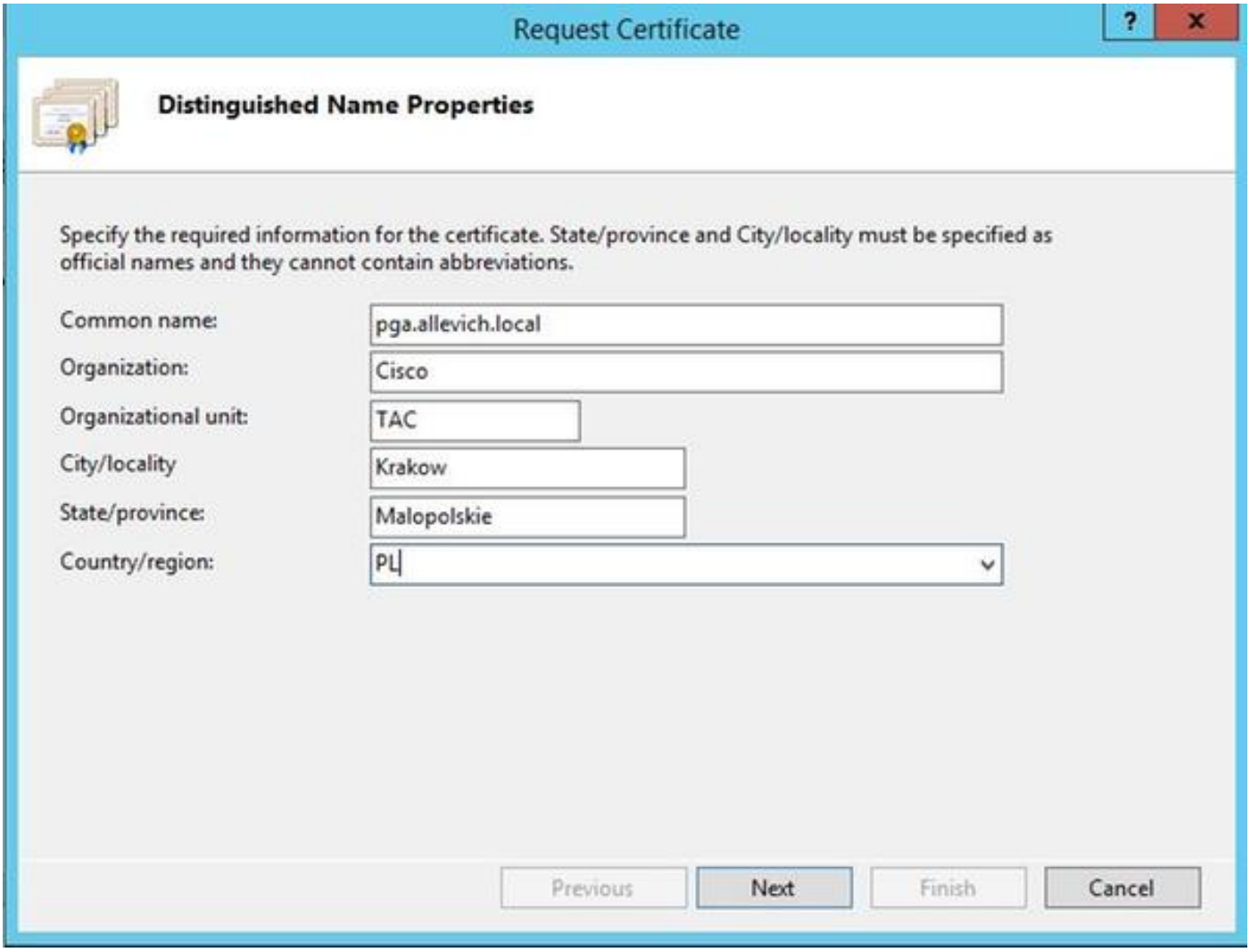
Открытый Менеджер информационных сервисов интернета (IIS), выберите свой узел, Периферийный шлюз A (PGA) в примере и **Серверные сертификаты**.



Выберите **Create Certificate Request** в панели действий.



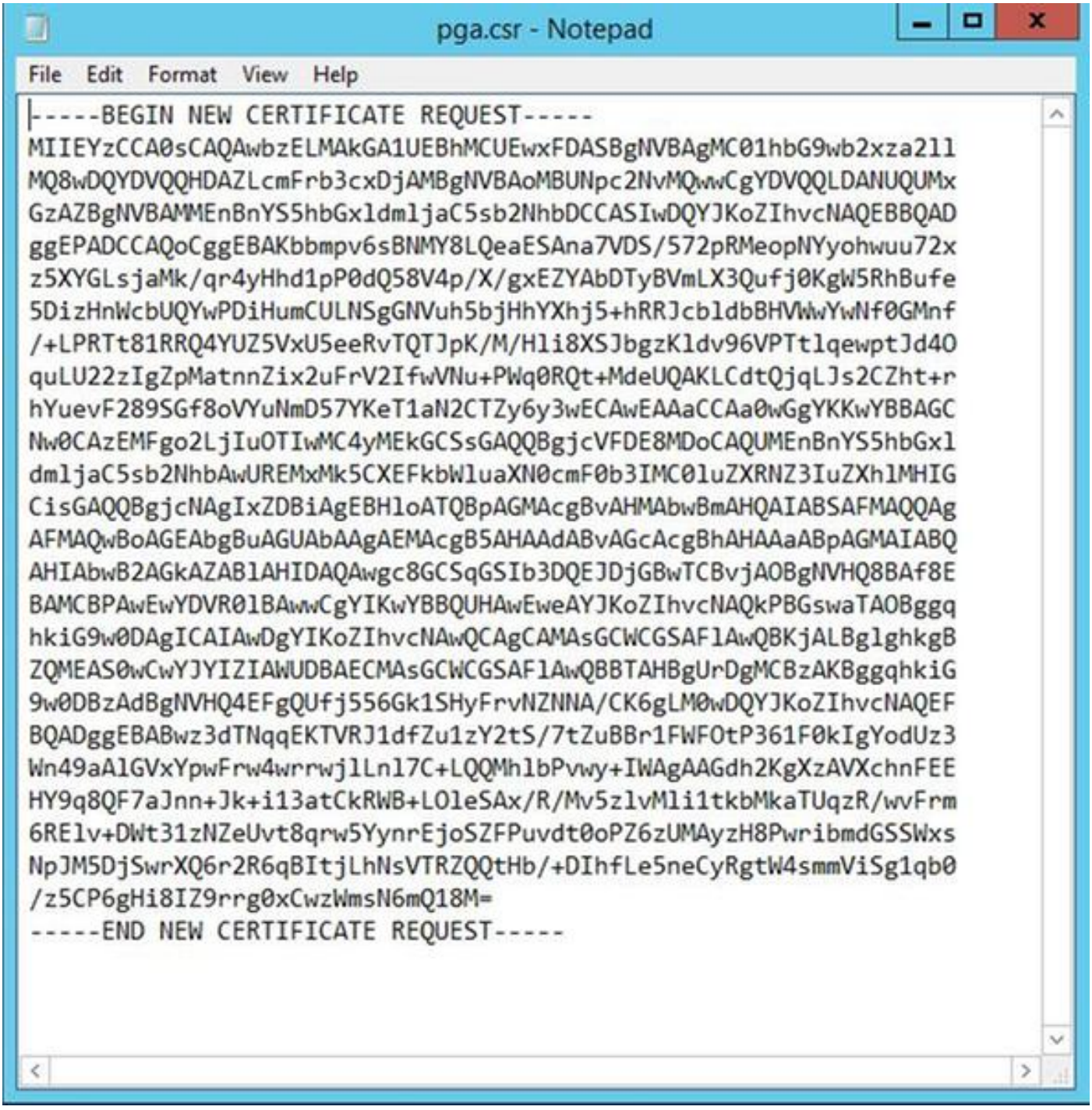
Введите **Общее имя (CN)**, **Организация** (O), **Организационная единица (OU)**, **Местность** (L), **Состояние** (ST), поля **Country (C)**. Общее имя должно совпасть с вашим именем хоста Полного доменного имени (FQDN) + доменное имя.



Оставьте настройки по умолчанию для провайдера криптографических служб и задайте длину в битах: 2048.

Выберите путь, где сохранить. Например, на рабочем столе с названием pga.csr.

Открытый недавно созданный запрос в блокноте.



Скопируйте сертификат в буфер с CTRL+C.

Подпишите сертификат на центре сертификации

> **Примечание:** При использовании внешнего центра сертификации (как GoDaddy), необходимо связаться с ними после генерации файла CSR.

Регистрируйтесь к своему серверному сертификату CA, регистрируют страницу.
https://<адрес сервера CA>/certsrv

Выберите **Request Certificate**, **Advanced Certificate Request** и вставьте содержание Запроса подписи сертификата (CSR) к буферу. Затем выберите **Certificate Template как Web-сервер**.

Ядро загрузки 64 закодировало сертификат.

Откройте сертификат и скопируйте содержание поля следа большого пальца для более позднего использования. Удалите пробелы из следа большого пальца.

Установите сертификат

Скопируйте сертификат

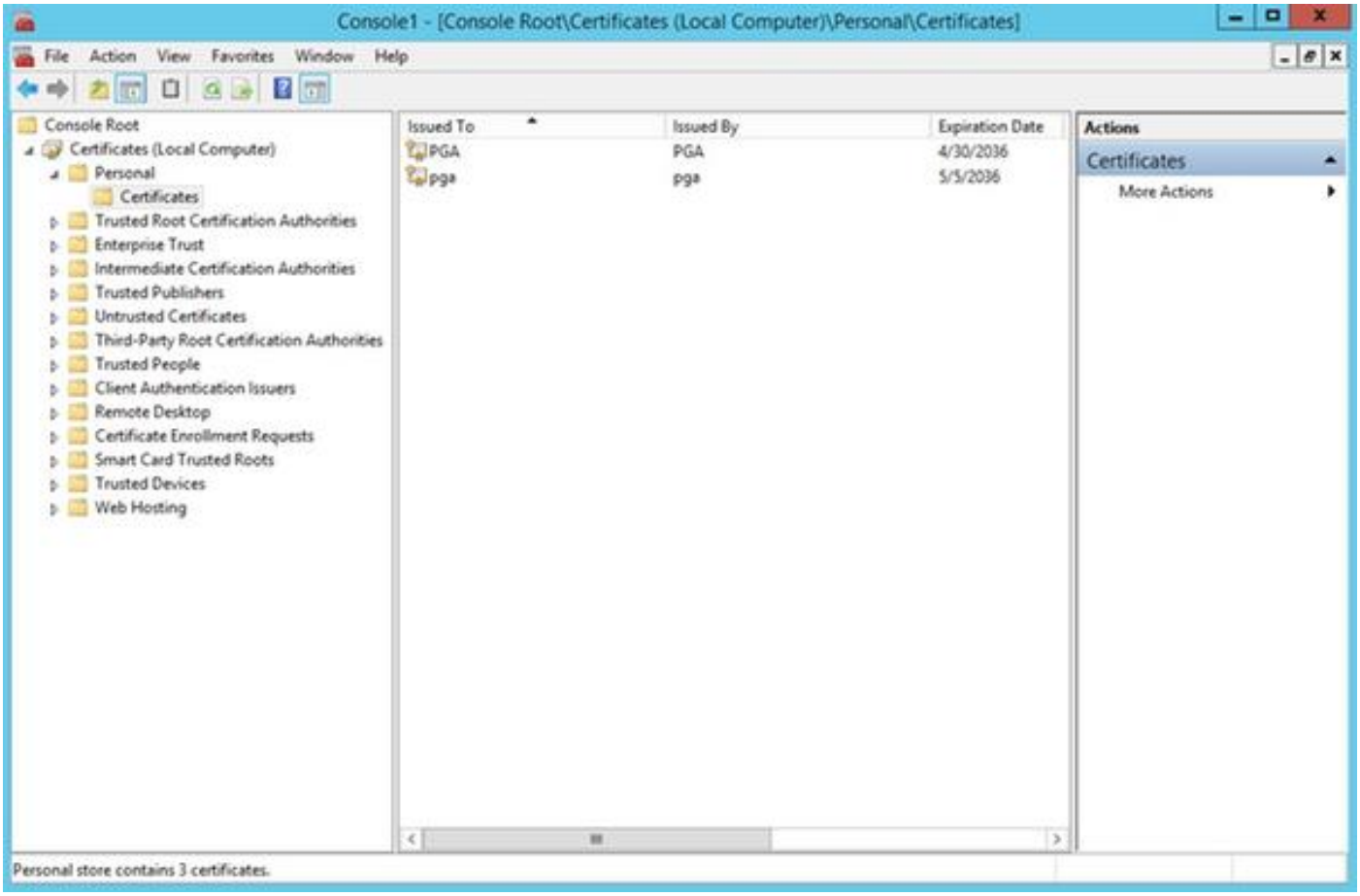
Скопируйте недавно генерируемый файл сертификата в VM UCCE, где расположено программное средство Портика.

Импортируйте сертификат в хранилище локального компьютера

На том же сервере UCCE запускают консоль Консоли управления Microsoft (MMC) путем выбора меню Пуск, вводят **выполненный** и **mmc**.

Нажмите **моментальный снимок Add/Remove - в**, и в диалоговом окне **нажмите Add**.
Затем выберите меню **Certificates** и добавьте.
В моментальном снимке Сертификатов - в диалоговом окне, нажмите **Computer Account> Local Computer> Finish**.

Перейдите к папке персональных сертификатов.



В действиях область выбирают **More Actions> All Tasks> Import**.

Нажмите Next, **Просмотрите** и выберите сертификат, который генерировался ранее, и в следующем меню гарантируют, что значение сертификата было придано к персональному. На последнем экранном verify **Хранилище Сертификата** и выбранном **Файле сертификата** и нажимают **Finish**.

Свяжите сертификат IIS

Открытое приложение cmd.

Переместитесь к Диагностическому Портику по домашней папке.

```
cd c:\icm\serviceability\diagnostics\bin
```

Удалите текущую привязку сертификата для программного средства Портика.

```
DiagFwCertMgr /task:UnbindCert
```

Свяжите подписанный сертификат CA.

> **Совет:** Используйте некоторый текстовый редактор (блокнот ++) для удаления пробелов в хэше.

Используйте хэш, сохраненный прежде с удаленными пробелами.

```
DiagFwCertMgr /task:BindCertFromStore /certhash:bc6bbe23b8b3a26d8446c252400f9264c5c30a29
```

В случае, если сертификат связан успешно, необходимо видеть подобную линию в выходных данных.

"Привязка сертификата ДОПУСТИМА"

Гарантируйте, что привязка сертификата была успешным использованием этой команды.

```
DiagFwCertMgr /task:ValidateCertBinding
```

Снова подобное сообщение должно быть отображено в выходных данных.

"Привязка сертификата ДОПУСТИМА"

> **Примечание:** DiagFwCertMgr по умолчанию будет использовать порт 7890.

Перезапустите Диагностический сервис Платформы.

```
sc stop "diagfwsvc"
sc start "diagfwsvc"
```

> **Совет:** Сервисный список и особенно имя сервиса Портика могут быть проверены через команду списка задач в программном средстве cmd.

```
tasklist /v
```

Проверка

Открытая страница Diagnostic Framework с помощью FQDN и это не должно вызывать предупреждающее сообщение сертификата.

Отступите план

В случае, если вы проиграли доступ к программному средству Портика, можно восстановить подписанный сертификат и добавить исключение.
Это может быть сделано с помощью этой команды.

```
DiagFwCertMgr /task:CreateAndBindCert
```

Устранение неполадок

Не используйте IP-адрес когда вход в систему к Диагностическому программному средству Портика Платформы. Вы все еще получаете предупреждение сертификата, потому что FQDN должен совпасть со значением, заданным в поле CN сертификата.

Проверьте, что все серверы синхронизируются с NTP source.

```
w32tm /monitor
```

При попытке использовать альтернативное имя субъекта (SAN), или Алгоритм цифровой подписи Эллиптической кривой (DSA EC) или 4096 сертификатов длины ключа - сначала изолирует это, это не является определенным для одной из этих функций.

Похожие статьи

UCCE\PCCE - Процедура, чтобы получить и загрузить Windows Server Self-Signed или Сертификат Центра сертификации (CA) на 2008 серверах

Настройте Подписанный сертификат CA через CLI в голосовой операционной системе (VOS) Cisco