

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

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Настройка](#)

[Генерируйте сертификат запрос со знаком](#)

[Подпишите сертификат на центре сертификации](#)

[Установите сертификат](#)

[Скопируйте сертификат](#)

[Импортируйте сертификат в хранилище локального компьютера](#)

[Свяжите сертификат IIS](#)

[Проверка](#)

[Отступите план](#)

[Устранение неполадок](#)

[Похожие статьи](#)

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:

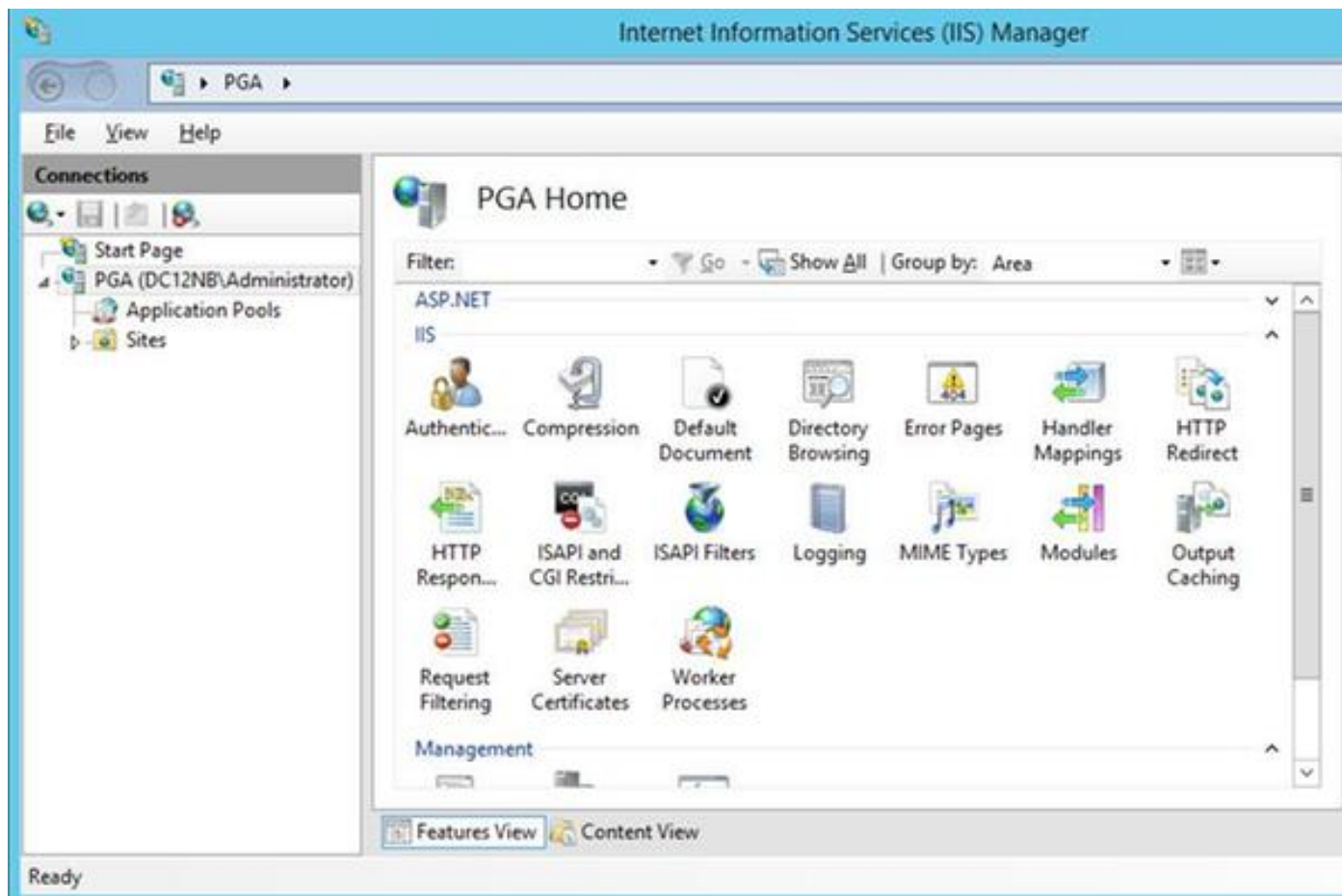
- Cisco UCCE 11.0.1
- Microsoft Windows server 2012 R2
- Центр сертификации R2 Microsoft Windows server 2012 года
- Microsoft Windows 7 SP1 ОС

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.

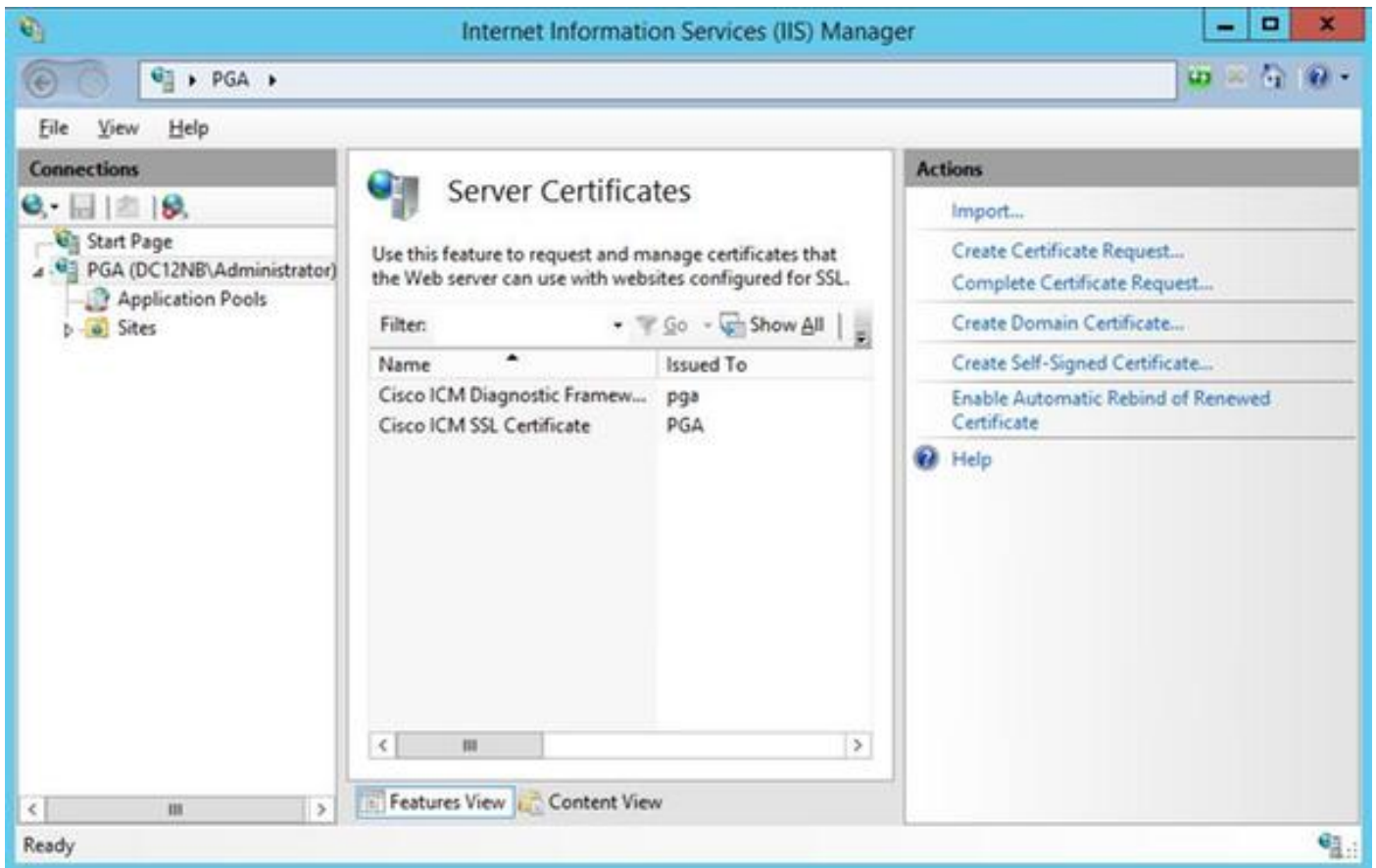
Настройка

Генерируйте сертификат запрос со знаком

Открытый Менеджер информационных сервисов интернета (IIS), выберите свой узел, Периферийный шлюз А (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.

Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	<input type="text" value="pga.allevich.local"/>
Organization:	<input type="text" value="Cisco"/>
Organizational unit:	<input type="text" value="TAC"/>
City/locality:	<input type="text" value="Krakow"/>
State/province:	<input type="text" value="Malopolskie"/>
Country/region:	<input type="text" value="PL"/>

Previous Next Finish Cancel

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.


```
pga.csr - Notepad
File Edit Format View Help
|-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEYzCCA0sCAQAwbzELMAKGA1UEBhMCUEwxFDASBgNVBAgMC01hbG9wb2xza211
MQ8wDQYDVQQHDAZLcmFr3cxDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANUQUx
GzAZBgNVBAMMEnBnYS5hbGxldm1jaC5sb2NhbDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAKbbmpv6sBNMY8LQeaESAna7VDS/572pRMeopNYyohwu72x
z5XYGLsjaMk/qr4yHhd1pP0dQ58V4p/X/gxEZYAbDTyBVmLX3Qufj0KgW5RhBufe
5DizHnWcbUQYwPDiHumCULNSgGNVuh5bjHhYXhj5+hRRJcb1dbBHVVwYwNf0GMnf
/+LPRTt81RRQ4YUZ5VxU5eeRvTQTJpK/M/H1i8XSJbgzK1dv96VPTt1qewptJd40
quLU22zIgZpMatnnZix2uFrV2IfwVNu+Pwq0RQt+MdeUQAKLCdtQjqLJs2CZht+r
hYuevF289SGf8oVYuNmD57YKeT1aN2CTZy6y3wECAwEAaCCAA0wGgYKKwYBBAGC
Nw0CAZEMFgo2LjIu0TIwMC4yMEkGCSsGAQQBgjcVFDE8MDoCAQUMEnBnYS5hbGx1
dmljaC5sb2NhbAwUREMxMk5CXEFkbWluaXN0cmF0b3IMC0luZXRNZ3IuZXh1MHIG
CisGAQQBgjcNAgIxZDBiAgEBHloATQBpAGMAcGvAHMAbwBmAHQAIABSAFMAQQAg
AFMAQwBoAGEAbgBuAGUAbAAgAEMAcb5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQ
AHIAbwB2AGkAZABIAHIDAQAawgc8GCSqGSIb3DQEJDDjGBwTCBvjA0BgNVHQ8BAf8E
BAMCBPAwEwYDVR01BAwwCgYIKwYBBQUHAwEweAYJKoZIhvcNAQkPBGswaTA0Bggq
hkiG9w0DAGICAIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAF1AwQBKjALBglghkgB
ZQMEAS0wCwYJYIZIAWUDBAECMA5GCWCGSAF1AwQBbTAHBgUrDgMCBzAKBggqhkiG
9w0DBzAdBgNVHQ4EFgQUfj556Gk1SHyFrvNZNNA/CK6gLM0wDQYJKoZIhvcNAQEF
BQADggEBABwz3dTnqqEKTVRJ1dfZu1zY2tS/7tZuBBn1FWF0tP361F0kIgYodUz3
Wn49aA1GVxYpwFrw4wrrwj1Ln17C+LQQMh1bPvwy+IWAgAAGdh2KgXzAVXchnFEE
HY9q8QF7aJnn+Jk+i13atCkRWB+L01eSAx/R/Mv5z1vM1i1tkbMkaTUqzR/wvFrm
6RElv+Dwt31zNZeUvt8qrw5YynrEjoSZFPuvdt0oPZ6zUMAYzH8PwribmdGSSWxs
NpJM5DjSwrXQ6r2R6qBItjLhNsVTRZQQtHb/+DIhfLe5neCyRgtW4smmViSg1qb0
/z5CP6gHi8IZ9rrg0xCwzWmsN6mQ18M=
-----END NEW CERTIFICATE REQUEST-----
```

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

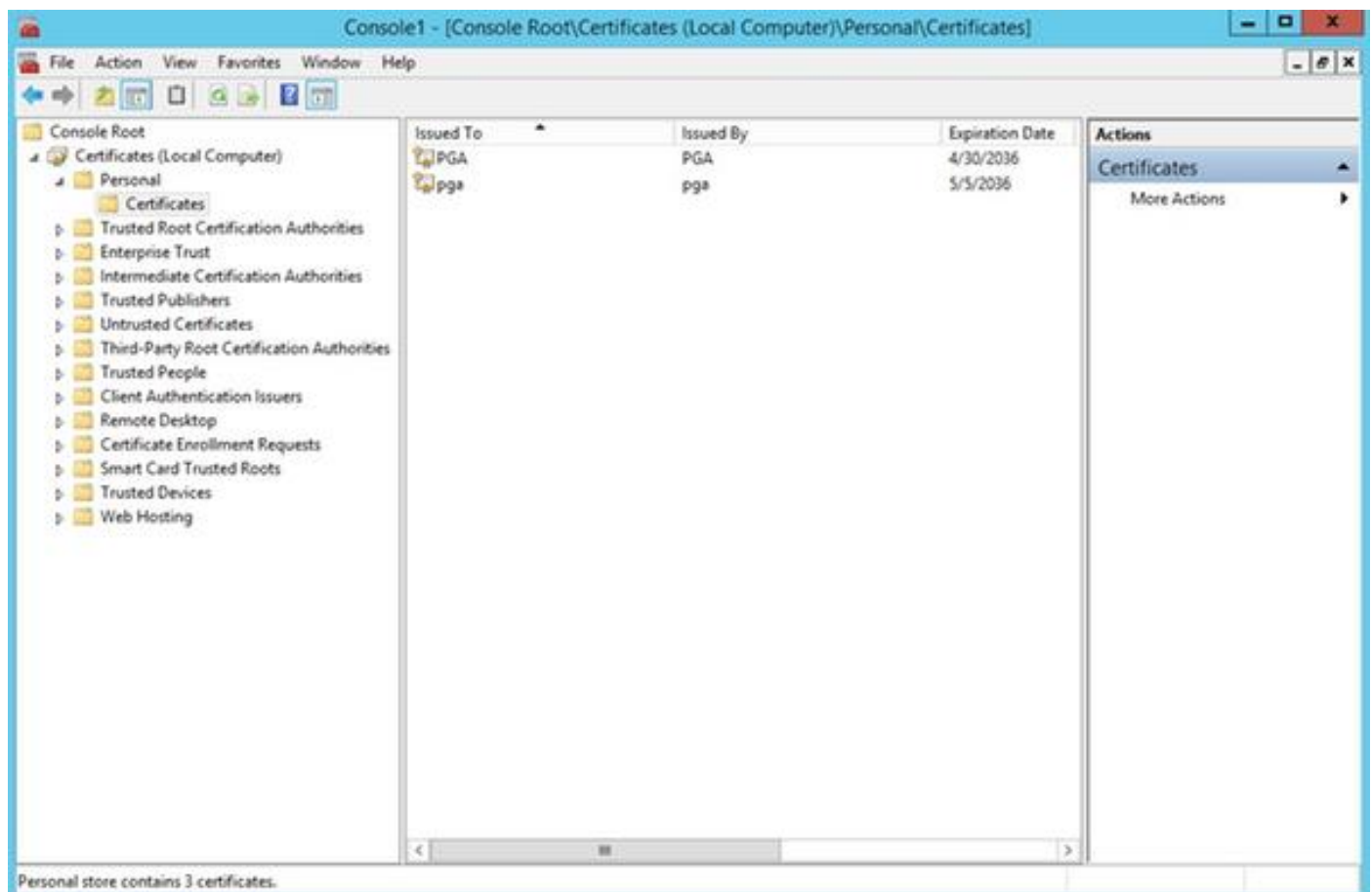
На том же сервере UCCE запускают консоль Консоли управления Microsoft (MMC) путем выбора меню Пуск, вводят **выполненный** и **mmc**.

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 Портника.

```
DiagFwCertMgr /task:UnbindCert
```

Свяжите подписанный сертификат СА.

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 Портника 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 Порттика, 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 Порттика 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](#)