

Установка бесплатного TLS/SSL сертификата Let's Encrypt в IIS/RDS в Windows Server

Клиент WACS для установки TLS сертификата Let's Encrypt в IIS на Windows Server

Самый простой способ получить SSL сертификат от Let's Encrypt — воспользоваться консольной утилитой **Windows ACME Simple (WACS)** (ранее проект назывался **LetsEncrypt-Win-Simple**). Она представляет собой простой мастер, который позволяет выбрать один из сайтов, запущенных на IIS, и автоматически выпустить и привязать к нему SSL сертификат.

Итак, предположим у нас имеется веб сайт на IIS, развёрнутый под управлением Windows Server 2016. Наша задача, переключить его в HTTPS режим, установив SSL сертификат от Let's Encrypt.

Скачайте последний релиз клиента WACS со страницы проекта на GitHub <https://github.com/PKISharp/win-acme/releases> (в моем случае это версия v2.0.10 – файл win-acme.v2.0.10.444.zip).

The screenshot shows the GitHub repository page for PKISharp/win-acme. The repository has 204 watches, 3,149 stars, and 525 forks. The 'Releases' tab is selected, showing the latest release v2.0.10, which was released 16 days ago by WouterTinus and has 451,005 downloads. Below the release information, there are sections for 'New features' and 'Support'. The 'Support' section includes a message about professional support and a link to a Patreon page. At the bottom, there is a table of assets for the release.

Asset	Size
win-acme.azure.v2.0.10.444.zip	342 KB
win-acme.dreamhost.v2.0.10.444.zip	4.52 KB
win-acme.route53.v2.0.10.444.zip	331 KB
win-acme.v2.0.10.444.zip	2.77 MB

Распакуйте архив в каталог на сервере с IIS: `c:\inetpub\letsencrypt`

Откройте командную строку с правами администратора, перейдите в каталог `c:\inetpub\letsencrypt` и запустите **wacs.exe**.

Запустится интерактивный мастер генерации сертификата Let's Encrypt и привязки его к сайту IIS. Чтобы быстро создать новый сертификат выберите **N**: — Create new certificates (simple for IIS).

```
Select Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd C:\inetpub\letsencrypt\
PS C:\inetpub\letsencrypt> .\wacs.exe

[INFO] A simple Windows ACMEv2 client (WACS)
[INFO] Software version 2.0.10.444 (RELEASE)
[INFO] IIS version 10.0
[WARN] Scheduled task not configured yet
[INFO] Please report issues at https://github.com/PKISharp/win-acme

N: Create new certificate (simple for IIS)
M: Create new certificate (full options)
L: List scheduled renewals
R: Renew scheduled
S: Renew specific
A: Renew *all*
O: More options...
Q: Quit

Please choose from the menu:
```

Затем нужно выбрать тип сертификата. В нашем примере нет необходимости использовать сертификат с псевдонимами (несколькими SAN — Subject Alternative Name), поэтому достаточно выбрать пункт **1. Single binding of an IIS site**. Если вам нужен Wildcard-сертификат, выберите опцию 3.

Далее утилита выведет список сайтов, запущенных на сервере IIS и предложит выбрать сайт, для которого нужно создать и привязать новый SSL сертификат.

```
Please specify how the list of domain names that will be included in the
certificate should be determined. If you choose for one of the "all bindings"
options, the list will automatically be updated for future renewals to reflect
the bindings at that time.

1: Single binding of an IIS website
2: All bindings of an IIS website
3: All bindings of multiple IIS websites
4: Manual input
5: Read a CSR created by another program
<Enter>: Abort

How shall we determine the domain(s) to include in the certificate?: 1

1:      e.com (SiteId 2)
<Enter>: Abort

Choose binding: 1
```

Укажите ваш email, на который будут отправляться уведомления о проблемах с обновлением сертификата сайта и другие о повешения (можно указать несколько email через запятую). Осталось согласится с условиями использования и Windows ACME Simple подключится к серверам Let's Encrypt и попытается автоматически сгенерировать новый SSL сертификат для вашего сайта.

```
[INFO] Target generated using plugin IISBinding: e.com
Enter email(s) for notifications about problems and abuse (comma seperated): admin@e.com
Terms of service: C:\ProgramData\win-acme\acme-v02.api.letsencrypt.org\LE-SA-v1.2-November-15-2017.pdf
Open in default application? (y/n*)
```

Процесс генерации и установки SSL сертификата Let's Encrypt для IIS полностью автоматизирован.

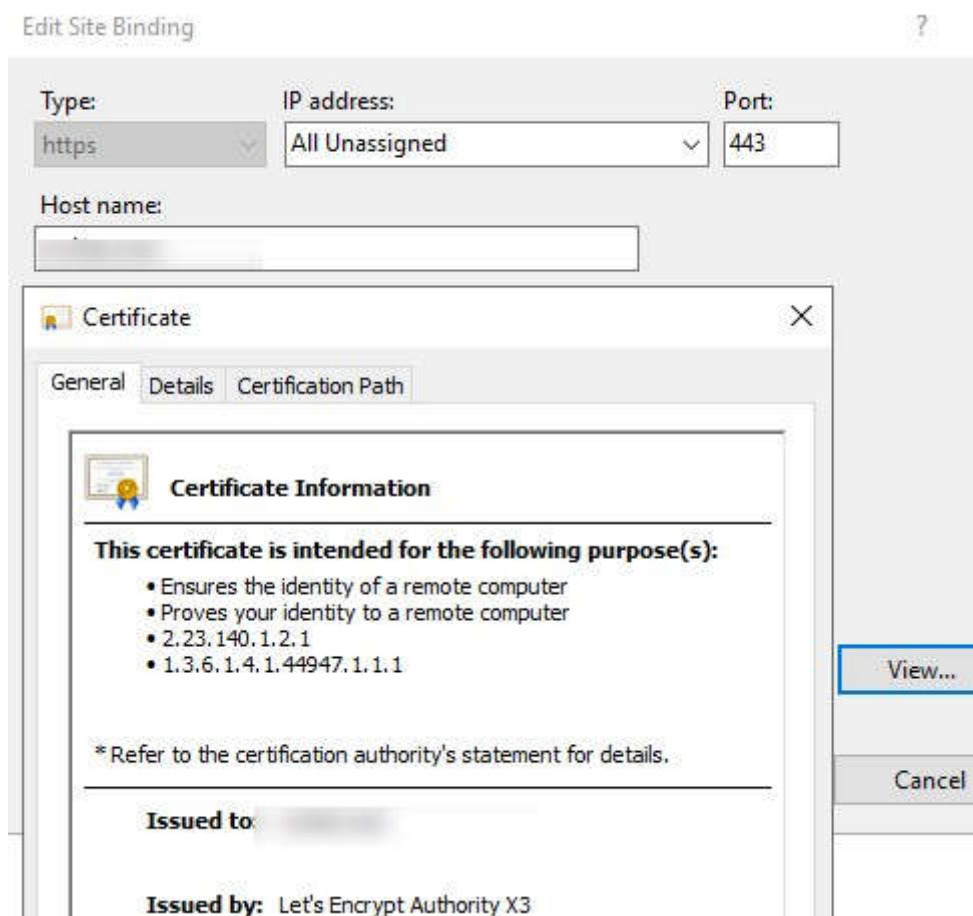
По умолчанию выполняется валидация домена в режиме **http-01 validation (SelfHosting)**. Для этого нужно, чтобы в DNS домена имелась запись, указывающая на ваш веб сервера. При

запуске WACS в ручном режиме можно выбрать валидацию типа — **4 [http-01]**
Create temporary application in IIS (recommended). В этом случае на веб-сервере IIS будет создано небольшое приложение, через которое сервера Let's Encrypt смогут провести валидацию.

Примечание. При выполнении TLS/HTTP проверки ваш сайт должен быть доступен снаружи по полному DNS имени по протоколам HTTP (80/TCP) и HTTPS (443/TCP).

Утилита WACS сохраняет закрытый ключ сертификата (*.pem), сам сертификат и ряд других файлов в каталог `C:\Users\%username%\AppData\Roaming\letsencrypt-win-simple`. Затем она в фоновом режиме установит сгенерированный SSL сертификат Let's Encrypt и привяжет его к вашему сайту IIS. Если на сайте уже установлен SSL сертификат (например, [самоподписанный](#)), он будет заменен новым.

В IIS Manager откройте меню **Site Binding** для вашего сайта и убедитесь, что для него используется сертификат, выданный *Let's Encrypt Authority X3*.



Windows ACME Simple создает новое правило в планировщике заданий Windows (**win-acme-renew (acme-v02.api.letsencrypt.org)**) для автоматического продления сертификата. Задание запускается каждый день, продление сертификата выполняется через 60 дней.

Планировщик запускает команду:

```
C:\inetpub\letsencrypt\wacs.exe --renew --baseuri "https://acme-v02.api.letsencrypt.org"
```

Эту же команду вы можете использовать для ручного обновления сертификата.

Task Scheduler

FileActionViewHelp

Task Scheduler (Local)

Task Scheduler Library

Microsoft

Name	Status	Triggers
win-acme renew (acme-v02.api.letsencrypt.org)	Ready	At 9:00 AM every day