

# How to Install a Let's Encrypt SSL/TLS Certificate on Windows Server 2019 with Internet Information Services (IIS)

Learn how to secure your website with a free Let's Encrypt SSL/TLS certificate on Windows Server 2019 using IIS in this step-by-step installation guide.

# Contents

01	Introduction	3
02	Install IIS	3
03	Create a Simple Web Application	4
04	Set Up an IIS Site with Your Domain	4
05	Request and Install a Let's Encrypt Certificate	6
06	Use Win-acme (Recommended)	6
07	Use Certbot with Manual Binding (Alternative)	7
08	Redirect HTTP Requests to HTTPS	8
09	Missing web.config?	10
010	Conclusion	11

# Introduction

---

Securing your web applications with HTTPS is essential for protecting data in transit and improving user trust. This article explains how to install a free Let's Encrypt SSL/TLS certificate on Windows Server using Internet Information Services (IIS).

In this article, you'll use the win-acme client to request and apply a certificate, bind it in IIS, and enable automatic HTTPS redirection. Optional instructions for Certbot and manual `.pfx` conversion are also included for advanced use cases.

## Install IIS

---

IIS is a built-in feature on Windows Server that you can enable using Server Manager.

1. Open **Server Manager** from the Start menu.
2. Click **Add Roles and Features**.
3. Choose **Role-based or feature-based installation**, then select your server.
4. On the **Server Roles** screen, check **Web Server (IIS)**.
5. Add any additional features you need, then click **Install**.
6. After installation, test the setup by visiting your public server IP in a browser:

```
http://YOUR-SERVER-IP
```

You should see the default IIS welcome page.

# Create a Simple Web Application

---

To verify that IIS is serving content correctly, create a basic HTML application:

1. Open **File Explorer** and create a folder for your website.
2. Press `Win + R`, type `notepad`, and press Enter.
3. Paste the following HTML code into Notepad:

```
HTML

<html>
  <head>
    <title>Hello World</title>
  </head>
  <body>
    <h1>Hello World!</h1>
  </body>
</html>
```

4. Save the file as `index.html` in the folder you just created.

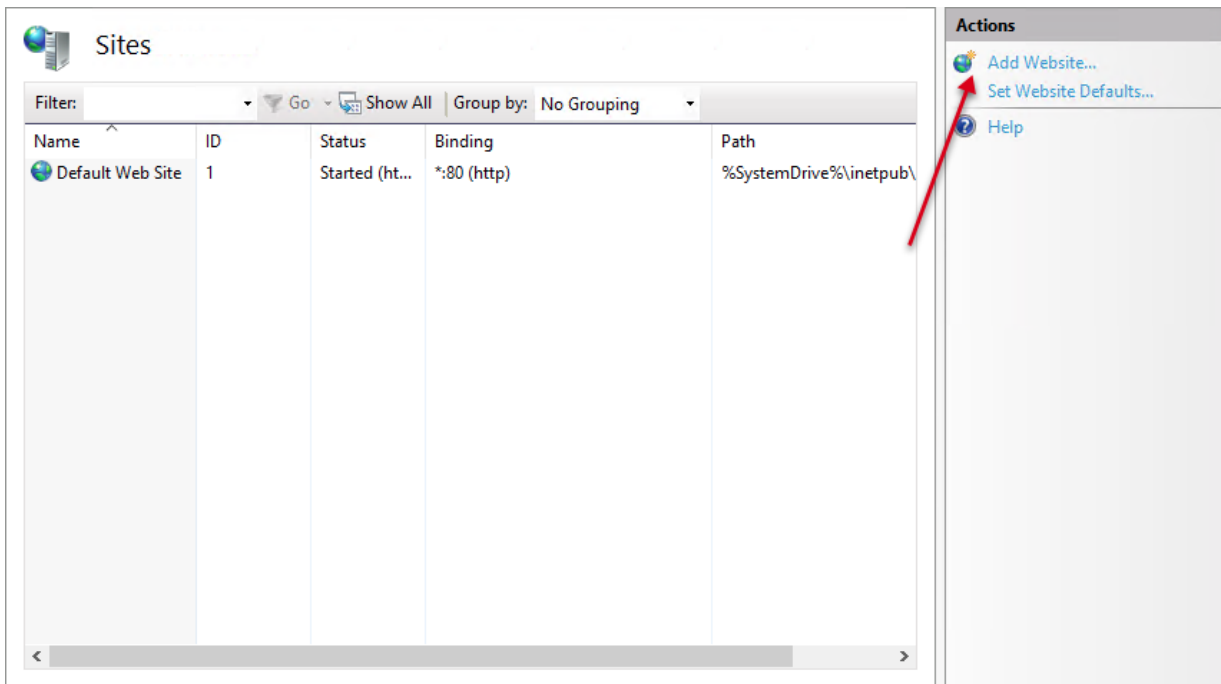
Next, you'll add this directory as a site in IIS and map it to your domain.

## Set Up an IIS Site with Your Domain

---

After creating your web files, configure a new IIS site that maps your domain to the correct folder.

1. Open **IIS Manager** from the Start Menu under **Windows Administrative Tools**.
2. In the **Connections** pane, expand your server name and right-click **Sites**, then select **Add Website**.



3. In the **Add Website** window, configure the following:

- **Site name:** Enter a name to identify the site internally (e.g., `example.com`).
- **Physical path:** Click `...` and select the folder you created earlier.
- **Binding:**
  - **Type:** Select `http`.
  - **IP address:** Leave as **All Unassigned** unless you're using a dedicated IP.
  - **Port:** Use `80`.
  - **Hostname:** Enter your domain name (e.g., `example.com`).

4. Click **OK** to create and start the site.

5. To verify the setup, open a browser and navigate to:

```
http://example.com
```

You should see the "Hello World" page you created earlier.

# Request and Install a Let's Encrypt Certificate

---

You can install a free SSL/TLS certificate from Let's Encrypt using one of two tools:

- **Win-acme** : Recommended for most users; installs directly into IIS and automates renewal.
- **Certbot** : More advanced; offers flexible control and cross-platform support.

Review both methods below and choose the one that best suits your workflow.

## Use Win-acme (Recommended)

---

**Win-acme** is a lightweight Let's Encrypt client that installs certificates directly into the IIS certificate store and configures HTTPS bindings automatically.

1. [Download the latest Win-acme zip archive](#).
2. Extract the contents and run `wacs.exe` as Administrator.
3. Click **More info** > **Run anyway** if SmartScreen appears.
4. When prompted, press **N** to create a new certificate.
5. Choose the site from the list that matches your IIS domain.
6. Press **A** to apply the certificate to all bindings.
7. Accept all defaults (**Y** to continue, open in IIS, agree to Let's Encrypt terms).
8. Enter your email address when prompted.

Win-acme automatically:

- Requests the certificate
- Stores it in the Windows certificate store
- Binds it to your IIS website
- Sets up automatic renewal

Once complete, visit `https://example.com` in a browser to verify HTTPS is active.

## Use Certbot with Manual Binding (Alternative)

[Certbot](#) is a versatile Let's Encrypt client that offers flexible control, but requires manual certificate binding in IIS.

### Install Certbot

1. [Download Certbot for Windows](#) and run the installer.
2. Open **PowerShell as Administrator** and run:

```
PWSH  
certbot -d example.com -m admin@example.com --agree-tos --  
webroot
```

Enter the site directory path when prompted.

This stores certificates as `.pem` files in:

```
C:\Certbot\live\example.com\
```

### Convert to `.pfx` Using OpenSSL

1. [Install OpenSSL for Windows](#).
2. Open PowerShell and navigate to OpenSSL's `bin` directory:

```
PWSH  
cd "C:\Program Files\OpenSSL-Win64\bin"
```

3. Convert your certificate to `.pfx` format:

PWSH

```
.\openssl.exe pkcs12 -export \  
-out C:\Certbot\live\example.com\certificate.pfx \  
-inkey C:\Certbot\live\example.com\privkey.pem \  
-in C:\Certbot\live\example.com\fullchain.pem
```

## Import and Bind the Certificate

1. Open **IIS Manager**.
2. Select the **server name**, then open **Server Certificates**.
3. Click **Import**, select your `.pfx` file, enter the password, and confirm.
4. Navigate to **Sites**, select your domain, and click **Bindings**.
5. Click **Add**, select `https`, and assign:
  - Port: `443`
  - Hostname: `example.com`
  - Certificate: Select from dropdown
6. Check **Require Server Name Indication** and confirm with **OK**.

Visit `https://example.com` to confirm your certificate is active.

## Redirect HTTP Requests to HTTPS

---

Use the **IIS URL Rewrite** module to automatically redirect all HTTP traffic to HTTPS.

### Install the URL Rewrite Module

1. [Download the URL Rewrite module](#).
2. Run the installer and complete the setup.
3. Open **IIS Manager**, click your server name, and confirm that **URL Rewrite** is available in **Features View**.

### Create a Redirect Rule in IIS

1. In **IIS Manager**, expand your server and select your site under **Sites**.

2. Double-click **URL Rewrite**.
3. In the **Actions** pane, click **Add Rules**.
4. Under **Inbound Rules**, select **Blank rule** and click **OK**.
5. Name your rule (e.g., `Redirect to HTTPS`).
6. Keep **Requested URL** as `Matches the Pattern`, **Using** as `Regular Expressions`.
7. Set the **Pattern** to:

```
(.*)
```

8. Uncheck **Ignore case**.

#### Add a Condition

1. Expand **Conditions** and click **Add**.
2. Set **Condition input** to:

```
{HTTPS}
```

3. Leave **Check if input string** as `Matches the Pattern`.
4. Set **Pattern** to:

```
^OFF$
```

5. Click **OK**.

#### Define Redirect Action

1. Scroll to **Action** settings and configure:
  - **Action type:** `Redirect`
  - **Redirect URL:**

```
https://{HTTP_HOST}{REQUEST_URI}
```

- Uncheck **Append query string**
- Set **Redirect type** to `Permanent (301)`

2. Click **Apply** in the **Actions** pane.

## Test the Redirect

Open your browser and visit:

```
http://example.com
```

You should be redirected to the HTTPS version automatically.

## Missing web.config?

If the redirect does not work, confirm that a `web.config` file exists in your site root. If missing, create one with the following content:

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <rewrite>
      <rules>
        <rule name="Redirect to HTTPS" stopProcessing="true">
          <match url="(.*)" />
          <conditions>
            <add input="{HTTPS}" pattern="^OFF$" />
          </conditions>
          <action type="Redirect" url="https://{HTTP_HOST}{REQUEST_URI}" appendQueryString="false" />
        </rule>
      </rules>
    </rewrite>
  </system.webServer>
</configuration>
```

```
</system.webServer>  
</configuration>
```

Save the file and re-test the redirect in your browser.

## Conclusion

---

In this article, you learned how to secure a website hosted on Internet Information Services (IIS) with a free Let's Encrypt SSL/TLS certificate on Windows Server. You set up IIS, deployed a basic web application, installed the certificate using Certbot or win-acme, configured HTTPS bindings, and redirected HTTP traffic to HTTPS.

With SSL properly configured, your server is now ready for secure web hosting. To build on this setup, you can [install WordPress on IIS](#) or [set up PHP Manager](#) to support dynamic web applications.



VULTR

