
🔹 Configure Certificates & TLS for Azure App Service

TLS (Transport Layer Security) ensures encrypted communication (HTTPS) between clients and your web app. In Azure App Service, you can configure certificates and enforce TLS in just a few steps.

Step 1: Navigate to Your App Service

1. Log in to Azure Portal.
2. Go to **App Services** → select your web app.

Step 2: Add a Custom Domain (if needed)

- If you want to use a **custom domain** (e.g., `www.mydomain.com` instead of `*.azurewebsites.net`), configure it first:
    1. In App Service → **Custom domains**.
    2. Add your domain name.
    3. Update DNS records with your registrar (CNAME or A record + TXT verification).

(If you are fine using the default `azurewebsites.net`, you can skip this.)

Step 3: Configure Certificates

Azure App Service supports multiple ways to add certificates:

🔹 Option A: Free App Service Managed Certificate

1. Go to **TLS/SSL Settings** → **Certificates** → **Create App Service Managed Certificate**.
2. Select the custom domain you want to secure.
3. Click **Create**.
4. This issues a free SSL certificate (only for custom domains, not wildcard or root domains).

🔹 Option B: Upload Your Own Certificate

1. Go to **TLS/SSL Settings** → **Private Key Certificates (.pfx)**.
2. Click **Upload Certificate**.
3. Choose the `.pfx` certificate file, enter the password, and upload.
4. Once uploaded, assign it to your custom domain (next step).

🔹 Option C: Use Azure Key Vault Certificate

1. Store your SSL certificate in **Azure Key Vault**.
2. In **TLS/SSL Settings** → select **Key Vault References**.
3. Grant your App Service access to Key Vault (via Managed Identity).
4. Bind the certificate to your domain.

Step 4: Bind the Certificate

1. Go to **TLS/SSL Bindings** (inside **TLS/SSL Settings**).
2. Click **Add TLS/SSL Binding**.
3. Select:

- **Custom Domain**: Choose the domain (e.g., `www.mydomain.com`).
- **Certificate**: Select the uploaded/managed certificate.
- **TLS/SSL Type**: Choose **SNI SSL** (cheaper, multiple certs per IP) or **IP SSL** (dedicated IP, single cert).

4. Click **Add Binding**.

Step 5: Enforce HTTPS and TLS Version

1. In App Service → **TLS/SSL Settings**.
   - Under **Protocol Settings**, choose the minimum TLS version (Recommended: **TLS 1.2**).
   - Under **HTTPS Only**, switch to **On** (forces all traffic to HTTPS).
2. Save changes.

Step 6: Verify

1. Open your app URL with `https://`.
2. Check the certificate (browser padlock → view certificate).
3. Confirm TLS version using tools like SSL Labs Test.

Best Practices

- Always enforce **HTTPS** and minimum **TLS 1.2**.

- Use **App Service Managed Certificates** for free SSL if you don’t need advanced features.
- For production, consider **Azure Key Vault** to manage certificates automatically.
- Set **Auto-Renewal** for certificates to avoid expiry issues.

✅ **Summary:**

1. Add a custom domain.
2. Get a certificate (Free Managed / Upload / Key Vault).
3. Bind it to the domain in App Service.
4. Enforce HTTPS and TLS 1.2+.
