

[Azure](#) / [App Service](#) / [Web Apps](#) /

# Secure a custom DNS name with a TLS/SSL binding in Azure App Service

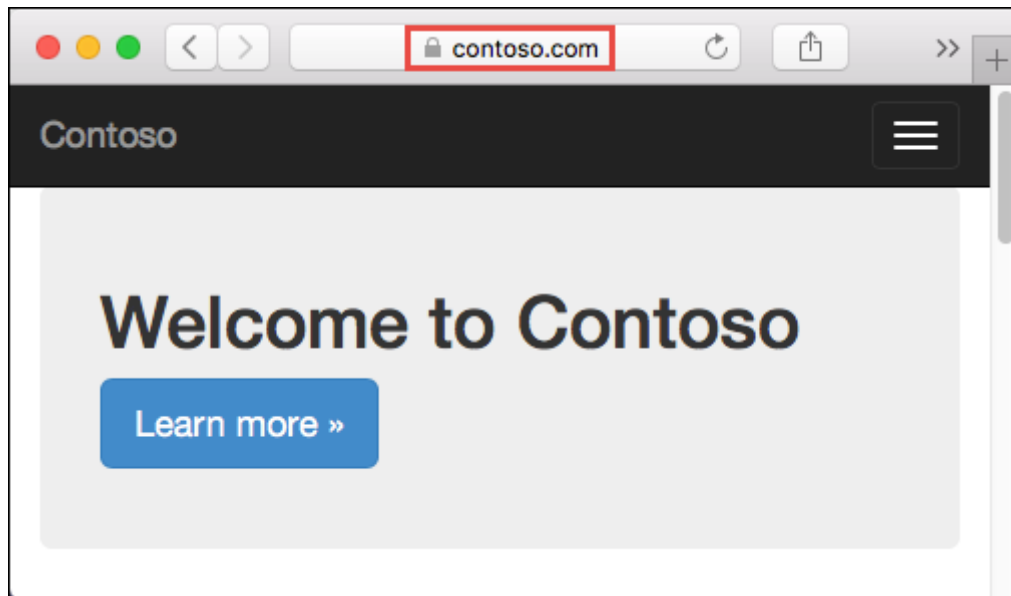
Article • 04/27/2022 • 7 minutes to read • [8 contributors](#)



## In this article

[Prerequisites](#)[Prepare your web app](#)[Secure a custom domain](#)[Remap records for IP SSL](#)[Test HTTPS](#)[Prevent IP changes](#)[Enforce HTTPS](#)[Enforce TLS versions](#)[Handle TLS termination](#)[Automate with scripts](#)[More resources](#)

This article shows you how to secure the [custom domain](#) in your [App Service app](#) or [function app](#) by creating a certificate binding. When you're finished, you can access your App Service app at the `https://` endpoint for your custom DNS name (for example, `https://www.contoso.com`).



Securing a [custom domain](#) with a certificate involves two steps:

- [Add a private certificate to App Service](#) that satisfies all the [private certificate requirements](#).
- Create a TLS binding to the corresponding custom domain. This second step is covered by this article.

In this tutorial, you learn how to:

- ✓ Upgrade your app's pricing tier
- ✓ Secure a custom domain with a certificate
- ✓ Enforce HTTPS
- ✓ Enforce TLS 1.1/1.2
- ✓ Automate TLS management with scripts

## Prerequisites

To follow this how-to guide:

- [Create an App Service app](#)
- [Map a domain name to your app](#) or [buy and configure it in Azure](#)
- [Add a private certificate to your app](#)

### ⓘ Note

The easiest way to add a private certificate is to **create a free App Service managed certificate**.

# Prepare your web app

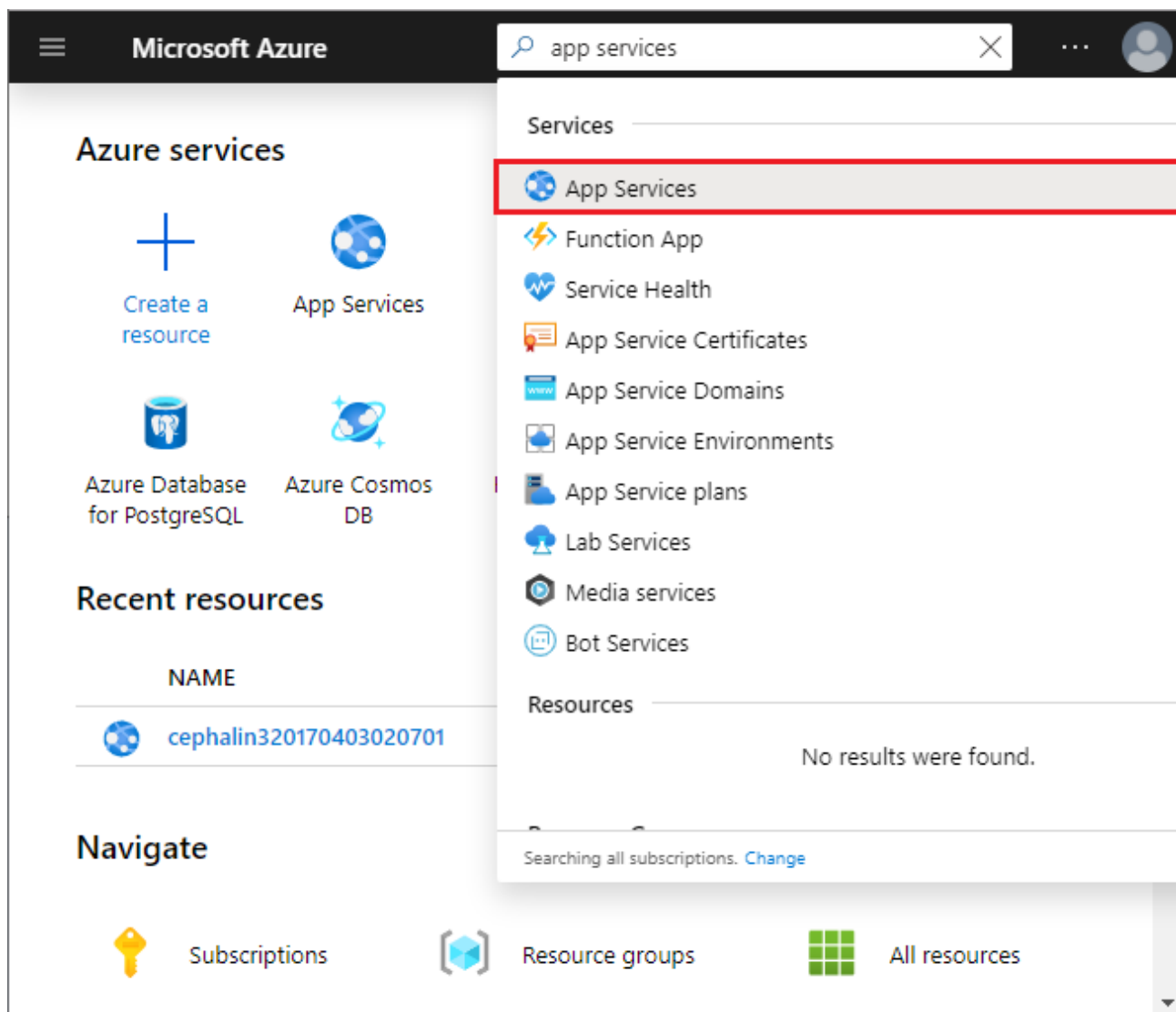
To create custom TLS/SSL bindings or enable client certificates for your App Service app, your [App Service plan](#) must be in the **Basic**, **Standard**, **Premium**, or **Isolated** tier. In this step, you make sure that your web app is in the supported pricing tier.

## Sign in to Azure

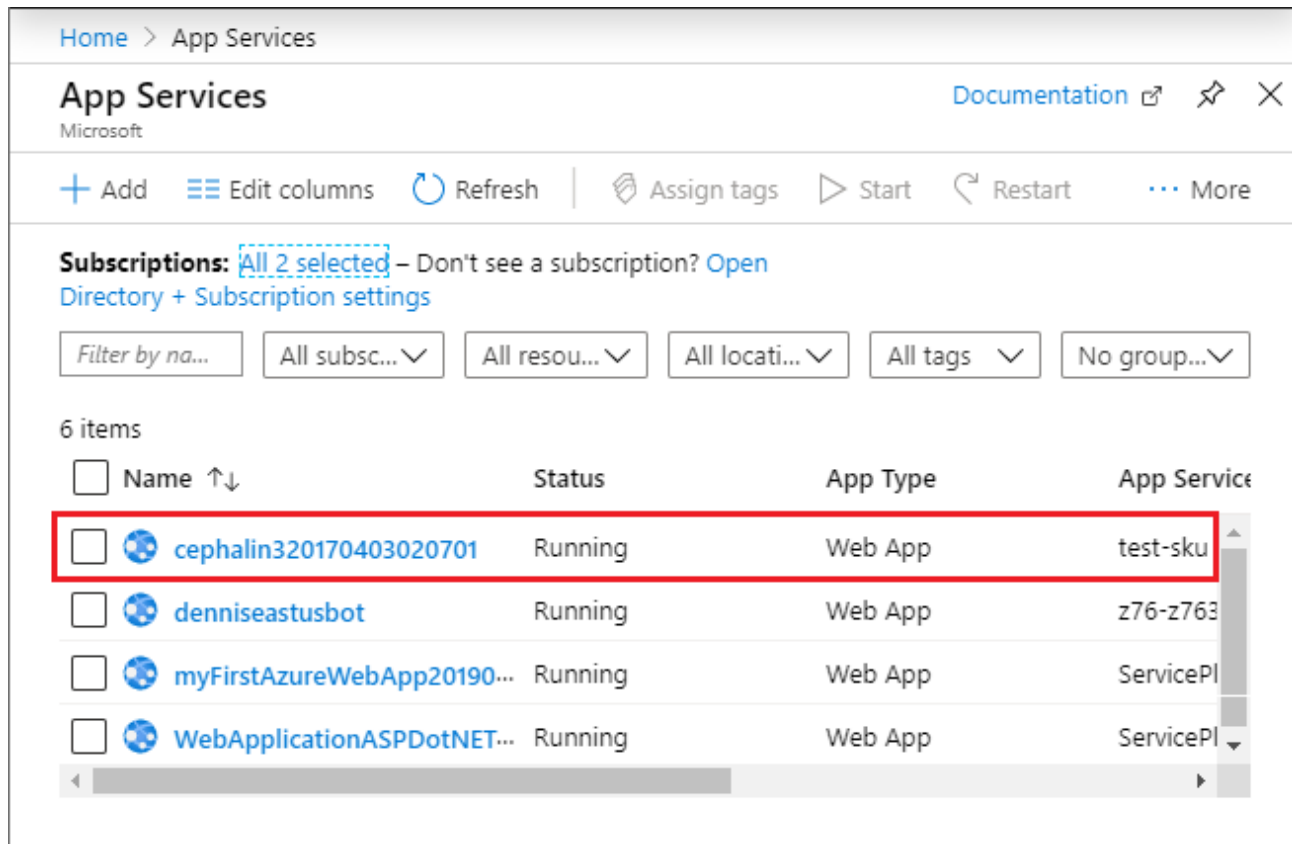
Open the [Azure portal](#) .

## Navigate to your web app

Search for and select **App Services**.



On the **App Services** page, select the name of your web app.



Home > App Services





**App Services** [Documentation](#)

+ Add Edit columns Refresh Assign tags Start Restart More

**Subscriptions:** All 2 selected – Don't see a subscription? [Open](#)  
[Directory + Subscription settings](#)

Filter by na... All subsc... All resou... All locati... All tags No group...

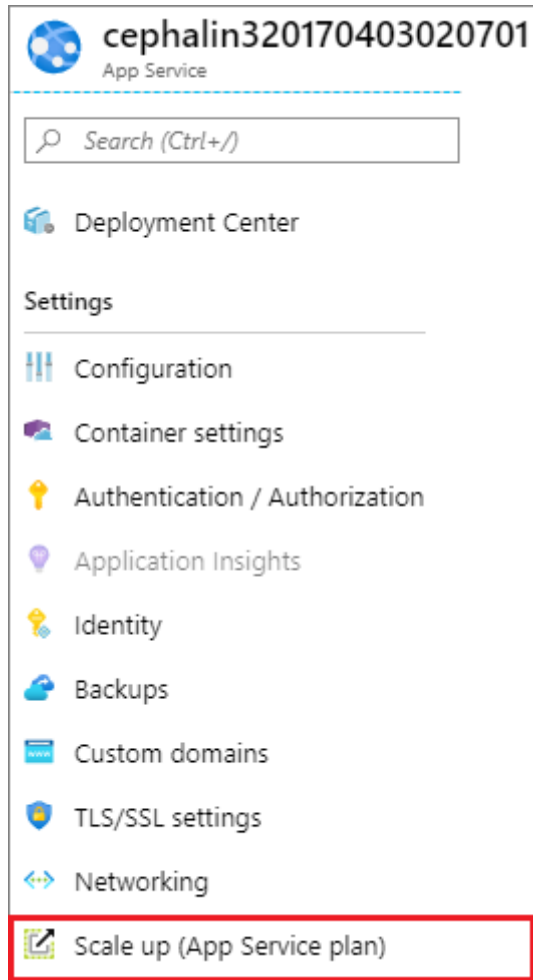
6 items

<input type="checkbox"/>	Name ↑↓	Status	App Type	App Service
<input type="checkbox"/>	 cephalin320170403020701	Running	Web App	test-sku
<input type="checkbox"/>	 denniseastusbot	Running	Web App	z76-z763
<input type="checkbox"/>	 myFirstAzureWebApp20190...	Running	Web App	ServicePl
<input type="checkbox"/>	 WebApplicationASPDotNET...	Running	Web App	ServicePl




You have landed on the management page of your web app.

## Check the pricing tier

In the left-hand navigation of your web app page, scroll to the **Settings** section and select **Scale up (App Service plan)**.



Check to make sure that your web app is not in the **F1** or **D1** tier. Your web app's current tier is highlighted by a dark blue box.

 <b>Dev / Test</b> For less demanding workloads	 <b>Production</b> For most production workloads	 <b>Isolated</b> Advanced networking and scale
---	--	--

### Recommended pricing tiers

**F1**  
Shared infrastructure  
1 GB memory  
60 minutes/day compute  
Free


**D1**  
Shared infrastructure  
1 GB memory  
240 minutes/day compute  
<price>/Month (Estimated)


**B1**  
100 total ACU  
1.75 GB memory  
A-Series compute equivalent  
<price>/Month (Estimated)

[See additional options](#)

### Included hardware

Every instance of your App Service plan will include the following hardware configuration:

**Azure Compute Units (ACU)**  
Dedicated compute resources used to run applications deployed in the App...

**Memory**  
Memory available to run applications

Custom SSL is not supported in the **F1** or **D1** tier. If you need to scale up, follow the steps in the next section. Otherwise, close the **Scale up** page and skip the [Scale up your App Service plan](#) section.

## Scale up your App Service plan

Select any of the non-free tiers (**B1**, **B2**, **B3**, or any tier in the **Production** category). For additional options, click **See additional options**.

Click **Apply**.

**Dev / Test**  
For less demanding workloads

**Production**  
For most production workloads

**Isolated**  
Advanced networking and scale

### Recommended pricing tiers

**F1**  
Shared infrastructure  
1 GB memory  
60 minutes/day compute  
Free

**D1**  
Shared infrastructure  
1 GB memory  
240 minutes/day compute  
<price>/Month (Estimated)

**B1**  
100 total ACU  
1.75 GB memory  
A-Series compute equivalent  
<price>/Month (Estimated)

[See additional options](#)

#### Included features

Every app hosted on this App Service plan will have access to these features:

**Custom domains / SSL**  
Configure and purchase custom domains with SNI SSL bindings

**Manual scale**  
Up to 3 instances. Subject to availability.

#### Included hardware

Every instance of your App Service plan will include the following hardware configuration:

**Azure Compute Units (ACU)**  
Dedicated compute resources used to run applications deployed in the App...

**Memory**  
Memory per instance available to run applications deployed and running in...

**Storage**  
10 GB disk storage shared by all apps deployed in the App Service plan.

**Apply**

When you see the following notification, the scale operation is complete.

Updating App Service Plan
3:14 PM

The plan 'Default1' was updated successfully!

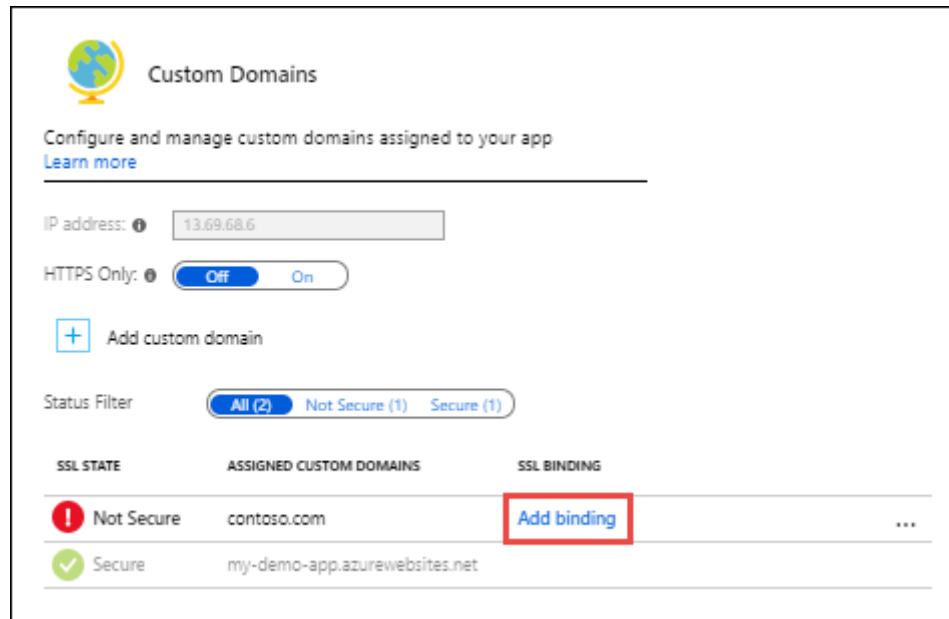
# Secure a custom domain

Do the following steps:

In the [Azure portal](#) , from the left menu, select **App Services** > <app-name>.

From the left navigation of your app, start the **TLS/SSL Binding** dialog by:

- Selecting **Custom domains** > **Add binding**
- Selecting **TLS/SSL settings** > **Add TLS/SSL binding**



In **Custom Domain**, select the custom domain you want to add a binding for.

If your app already has a certificate for the selected custom domain, go to [Create binding](#) directly. Otherwise, keep going.

## Add a certificate for custom domain

If your app has no certificate for the selected custom domain, then you have two options:

- **Upload PFX Certificate** - Follow the workflow at [Upload a private certificate](#), then select this option here.
- **Import App Service Certificate** - Follow the workflow at [Import an App Service certificate](#), then select this option here.

### Note





You can also **Create a free certificate** or **Import a Key Vault certificate**, but you must do it separately and then return to the **TLS/SSL Binding** dialog.

## Create binding

Use the following table to help you configure the TLS binding in the **TLS/SSL Binding** dialog, then click **Add Binding**.

Setting	Description
Custom domain	The domain name to add the TLS/SSL binding for.
Private Certificate Thumbprint	The certificate to bind.
TLS/SSL Type	<ul style="list-style-type: none"><li><b>SNI SSL</b> - Multiple SNI SSL bindings may be added. This option allows multiple TLS/SSL certificates to secure multiple domains on the same IP address. Most modern browsers (including Internet Explorer, Chrome, Firefox, and Opera) support SNI (for more information, see <a href="#">Server Name Indication</a> ).</li><li><b>IP SSL</b> - Only one IP SSL binding may be added. This option allows only one TLS/SSL certificate to secure a dedicated public IP address. After you configure the binding, follow the steps in <a href="#">Remap records for IP SSL</a>. IP SSL is supported only in <b>Standard</b> tier or above.</li></ul>

Once the operation is complete, the custom domain's TLS/SSL state is changed to **Secure**.

Status Filter		
<span>All (2)</span> <span>Not Secure (0)</span> <span>Secure (2)</span>		
SSL STATE	ASSIGNED CUSTOM DOMAINS	SSL BINDING
 Secure	contoso.com	SNI SSL ...
 Secure	my-demo-app.azurewebsites.net	

### ⓘ Note

A **Secure** state in the **Custom domains** means that it is secured with a certificate, but App Service doesn't check if the certificate is self-signed or expired, for example, which can also cause browsers to show an error or warning.

# Remap records for IP SSL

If you don't use IP SSL in your app, skip to [Test HTTPS for your custom domain](#).

There are two changes you need to make, potentially:

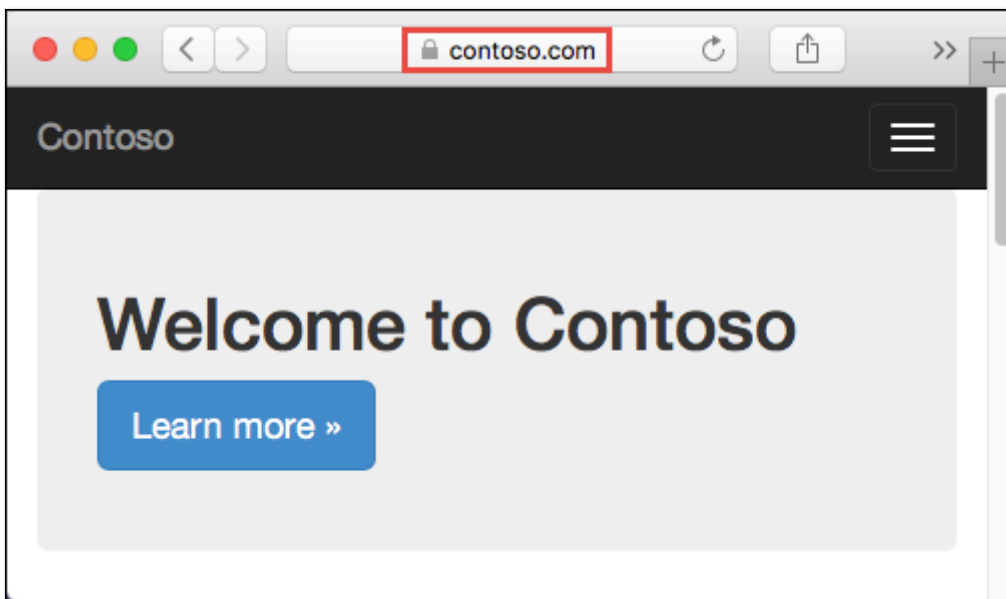
- By default, your app uses a shared public IP address. When you bind a certificate with IP SSL, App Service creates a new, dedicated IP address for your app. If you mapped an A record to your app, update your domain registry with this new, dedicated IP address.

Your app's **Custom domain** page is updated with the new, dedicated IP address. [Copy this IP address](#), then [remap the A record](#) to this new IP address.

- If you have an SNI SSL binding to `<app-name>.azurewebsites.net`, [remap any CNAME mapping](#) to point to `sni.<app-name>.azurewebsites.net` instead (add the `sni` prefix).

## Test HTTPS

In various browsers, browse to `https://<your.custom.domain>` to verify that it serves up your app.



Your application code can inspect the protocol via the "x-appservice-proto" header. The header will have a value of `http` or `https`.

### ⓘ Note

If your app gives you certificate validation errors, you're probably using a self-signed certificate.

If that's not the case, you may have left out intermediate certificates when you export your certificate to the PFX file.

## Prevent IP changes

Your inbound IP address can change when you delete a binding, even if that binding is IP SSL. This is especially important when you renew a certificate that's already in an IP SSL binding. To avoid a change in your app's IP address, follow these steps in order:

1. Upload the new certificate.
2. Bind the new certificate to the custom domain you want without deleting the old one.  
This action replaces the binding instead of removing the old one.
3. Delete the old certificate.

## Enforce HTTPS

By default, anyone can still access your app using HTTP. You can redirect all HTTP requests to the HTTPS port.

In your app page, in the left navigation, select **TLS/SSL settings**. Then, in **HTTPS Only**, select **On**.

When the operation is complete, navigate to any of the HTTP URLs that point to your app. For example:

- `http://<app_name>.azurewebsites.net`
- `http://contoso.com`
- `http://www.contoso.com`

## Enforce TLS versions

Your app allows [TLS 1.2](#) by default, which is the recommended TLS level by industry standards, such as [PCI DSS](#) . To enforce different TLS versions, follow these steps:

In your app page, in the left navigation, select **TLS/SSL settings**. Then, in **TLS version**, select the minimum TLS version you want. This setting controls the inbound calls only.

When the operation is complete, your app rejects all connections with lower TLS versions.

## Handle TLS termination

In App Service, [TLS termination](#) happens at the network load balancers, so all HTTPS requests reach your app as unencrypted HTTP requests. If your app logic needs to check if the user requests are encrypted or not, inspect the X-Forwarded-Proto header.

Language specific configuration guides, such as the [Linux Node.js configuration](#) guide, shows you how to detect an HTTPS session in your application code.

## Automate with scripts

### Azure CLI

[Bind a custom TLS/SSL certificate to a web app](#)

### PowerShell

PowerShell	Copy
------------	------

```

$fqdn="<Replace with your custom domain name>"
$pfXPath="<Replace with path to your .PFX file>"
$pfPassword="<Replace with your .PFX password>"
$webappName="mywebapp$(Get-Random)"
$location="West Europe"

# Create a resource group.
New-AzResourceGroup -Name $webappName -Location $location

# Create an App Service plan in Free tier.
New-AzAppServicePlan -Name $webappName -Location $location `
-ResourceGroupName $webappName -Tier Free

# Create a web app.
New-AzWebApp -Name $webappName -Location $location -AppServicePlan $we-
bappName `
-ResourceGroupName $webappName

Write-Host "Configure a CNAME record that maps $fqdn to
$webappName.azurewebsites.net"
Read-Host "Press [Enter] key when ready ..."

# Before continuing, go to your DNS configuration UI for your custom do-
main and follow the
# instructions at https://aka.ms/appservicecustomdns to configure a
CNAME record for the
# hostname "www" and point it your web app's default domain name.

# Upgrade App Service plan to Basic tier (minimum required by custom SSL
certificates)
Set-AzAppServicePlan -Name $webappName -ResourceGroupName $webappName `
-Tier Basic

# Add a custom domain name to the web app.
Set-AzWebApp -Name $webappName -ResourceGroupName $webappName `
-HostNames @($fqdn,"$webappName.azurewebsites.net")

# Upload and bind the SSL certificate to the web app.
New-AzWebAppSSLBinding -WebAppName $webappName -ResourceGroupName $we-
bappName -Name $fqdn `
-CertificateFilePath $pfXPath -CertificatePassword $pfPassword -
SslState SniEnabled

```

## More resources

- [Use a TLS/SSL certificate in your code in Azure App Service](#)
- [FAQ : App Service Certificates](#)

# Recommended content

## [Tutorial: Map existing custom DNS name - Azure App Service](#)

Learn how to add an existing custom DNS domain name (vanity domain) to a web app, mobile app back end, or API app in Azure App Service.

## [Add and manage TLS/SSL certificates - Azure App Service](#)

Create a free certificate, import an App Service certificate, import a Key Vault certificate, or buy an App Service certificate in Azure App Service.

## [Inbound/Outbound IP addresses - Azure App Service](#)

Learn how inbound and outbound IP addresses are used in Azure App Service, when they change, and how to find the addresses for your app.

## [Configuration and management FAQs for Web Apps - Azure](#)

Answers frequently asked questions about configuration and management issues for Azure App Service.

## [Deploy content using FTP/S - Azure App Service](#)

Learn how to deploy your app to Azure App Service using FTP or FTPS. Improve website security by disabling unencrypted FTP.

## [Azure App Service access restrictions - Azure App Service](#)

Learn how to secure your app in Azure App Service by setting up access restrictions.

## [Troubleshoot domain and TLS/SSL certificates - Azure App Service](#)

Find solutions to the common problems that you might encounter when you configure a domain or TLS/SSL certificate in Azure App Service.

## [Clone app with PowerShell - Azure App Service](#)

Learn how to clone your App Service app to a new app using PowerShell. A variety of cloning scenarios are covered, including Traffic Manager integration.

Show more 