Connect Azure Front Door Premium to a storage static website with Private Link

Applies to: ✓ Front Door Premium

This article shows you how to configure Azure Front Door Premium tier to connect to your storage static website privately using the Azure Private Link service.

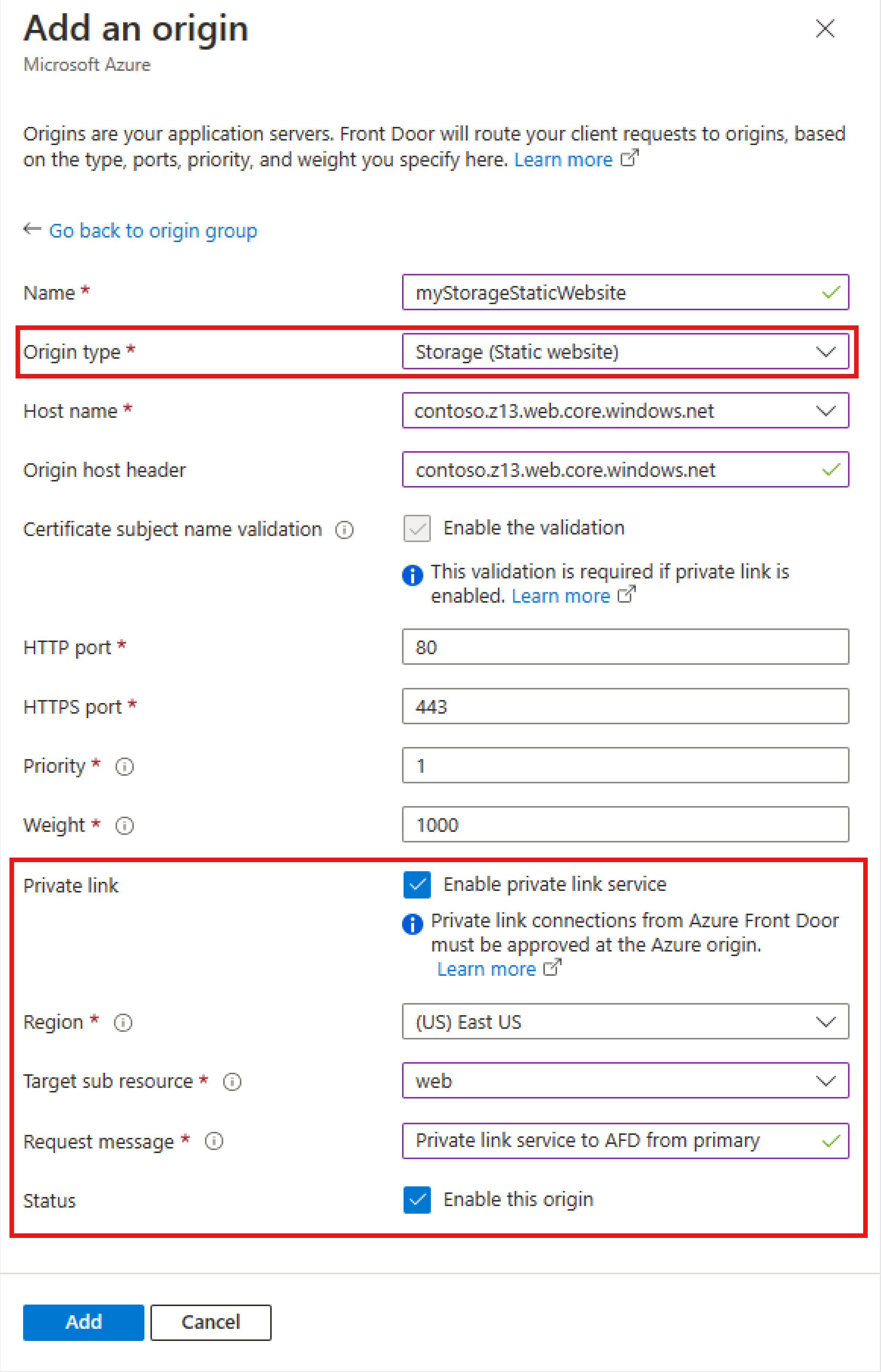
Prerequisites

- An Azure account with an active subscription. You can create an account for free .
- An Azure Front Door Premium profile with an origin group. For more information, see Create an Azure Front Door.
- A Private Link. For more information, see Create a Private Link service.
- Storage static website is enabled on your storage account. Learn how to enable static website.
- Sign in to the Azure portal with your Azure account.

Enable Private Link to a storage static website

In this section, you map the Private Link service to a private endpoint created in Azure Front Door's private network.

1. Sign in to the Azure portal .
2. Within your Azure Front Door Premium profile, under *Settings*, select **Origin groups**.
3. Select the origin group that contains the storage static website origin you want to enable Private Link for.
4. Select **+ Add an origin** to add a new storage static website origin or select a previously created storage static website origin from the list.



Add an origin

Microsoft Azure

Origins are your application servers. Front Door will route your client requests to origins, based on the type, ports, priority, and weight you specify here. Learn more

← Go back to origin group

Name *	myStorageStaticWebsite ✓
Origin type *	Storage (Static website)
Host name *	contoso.z13.web.core.windows.net
Origin host header	contoso.z13.web.core.windows.net ✓
Certificate subject name validation ⓘ	☑ Enable the validation ⓘ This validation is required if private link is enabled. Learn more
HTTP port *	80
HTTPS port *	443
Priority * ⓘ	1
Weight * ⓘ	1000
Private link	☑ Enable private link service ⓘ Private link connections from Azure Front Door must be approved at the Azure origin. Learn more
Region * ⓘ	(US) East US
Target sub resource * ⓘ	web
Request message * ⓘ	Private link service to AFD from primary ✓
Status	☑ Enable this origin

5. The following table has the information of what values to select in the respective fields while enabling private link with Azure Front Door. Select or enter the following settings to configure the storage static website you want Azure Front Door Premium to connect with privately.

Expand table

Setting	Value
Name	Enter a name to identify this storage static website origin.
Origin Type	Storage (Static website)
Host name	Select the host from the dropdown that you want as an origin.
Origin host header	You can customize the host header of the origin or leave it as default.
HTTP port	80 (default)
HTTPS port	443 (default)
Priority	Different origin can have different priorities to provide primary, secondary, and backup origins.
Weight	1000 (default). Assign weights to your different origin when you want to distribute traffic.
Region	Select the region that is the same or closest to your origin.
Target sub resource	The type of subresource for the resource selected previously that your private endpoint can access. You can select *web* or *web_secondary*.
Request message	Custom message to see while approving the Private Endpoint.

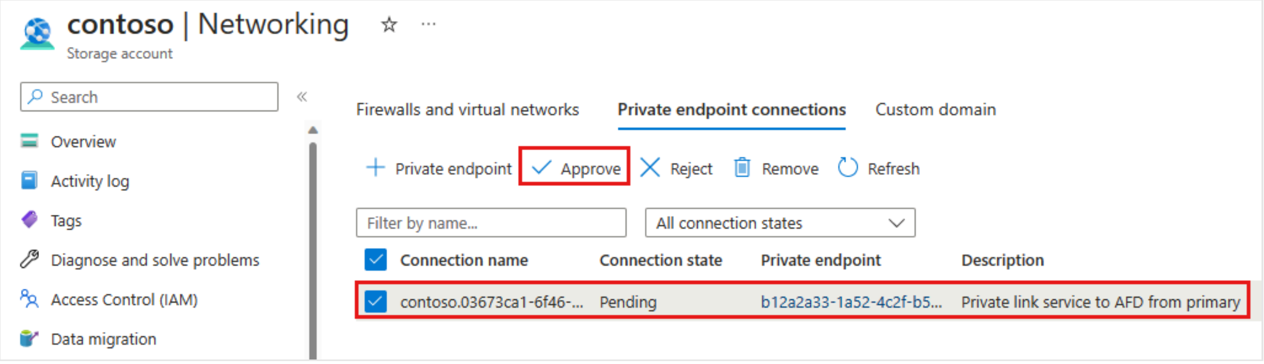
6. Then select **Add** to save your configuration. Then select **Update** to save your changes.

Approve private endpoint connection from storage account

1. Go to the storage account that you want to connect to Azure Front Door Premium privately. Select **Networking** under *Settings*.

2. In **Networking**, select **Private endpoint connections**.

3. Select the pending private endpoint request from Azure Front Door Premium then select **Approve**.

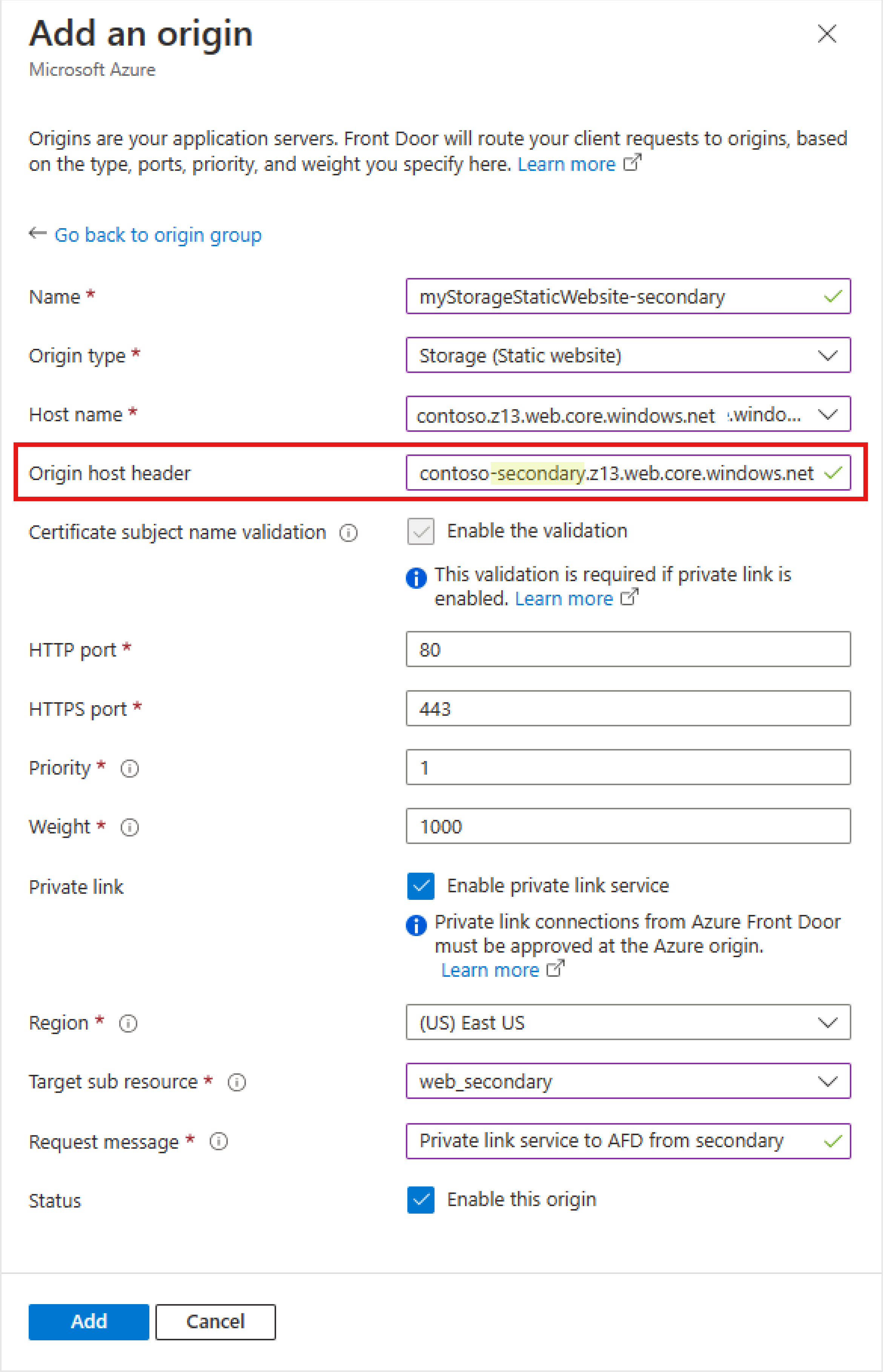


☑ Connection name	Connection state	Private endpoint	Description
☑ contoso.03673ca1-6f46-...	Pending	b12a2a33-1a52-4c2f-b5...	Private link service to AFD from primary

4. Once approved, you can see the private endpoint connection status is **Approved**.

Create private endpoint connection to web_secondary

When creating a private endpoint connection to the storage static website's secondary sub resource, you need to add a **-secondary** suffix to the origin host header. For example, if your origin host header is *contoso.z13.web.core.windows.net*, you need to change it to *contoso-secondary.z13.web.core.windows.net*.



Add an origin

Microsoft Azure

Origins are your application servers. Front Door will route your client requests to origins, based on the type, ports, priority, and weight you specify here. Learn more

← Go back to origin group

Name *	myStorageStaticWebsite-secondary ✓
Origin type *	Storage (Static website)
Host name *	contoso.z13.web.core.windows.net :.windo...
Origin host header	contoso-secondary.z13.web.core.windows.net ✓
Certificate subject name validation ⓘ	☑ Enable the validation This validation is required if private link is enabled. Learn more
HTTP port *	80
HTTPS port *	443
Priority * ⓘ	1
Weight * ⓘ	1000
Private link	☑ Enable private link service Private link connections from Azure Front Door must be approved at the Azure origin. Learn more
Region * ⓘ	(US) East US
Target sub resource * ⓘ	web_secondary
Request message * ⓘ	Private link service to AFD from secondary ✓
Status	☑ Enable this origin

Once the origin is added and the private endpoint connection is approved, you can test your private link connection to your storage static website.

Common mistakes to avoid

The following are common mistakes when configuring an origin with Azure Private Link enabled:

- Adding the origin with Azure Private Link enabled to an existing origin group that contains public origins. Azure Front Door doesn't allow mixing public and private origins in the same origin group.