



Windows PowerShell Get-Help on Cmdlet 'Enable-AzFrontDoorCustomDomainHttps'

PS: \>Get-HELP Enable-AzFrontDoorCustomDomainHttps -Full

NAME

Enable-AzFrontDoorCustomDomainHttps

SYNOPSIS

Enable HTTPS for a custom domain using Front Door managed certificate or using own certificate from Azure Key Vault.

SYNTAX

```

Enable-AzFrontDoorCustomDomainHttps [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -FrontDoorName
    <System.String> -FrontendEndpointName <System.String> [-MinimumTlsVersion <System.String>]
-ResourceGroupName <System.String> [-Confirm] [-WhatIf] [<CommonParameters>]

```

```

Enable-AzFrontDoorCustomDomainHttps [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -FrontDoorName
    <System.String> -FrontendEndpointName <System.String> [-MinimumTlsVersion <System.String>]
-ResourceGroupName <System.String> -SecretName <System.String>
[-SecretVersion <System.String>] -VaultId <System.String> [-Confirm] [-WhatIf] [<CommonParameters>]

```

<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -InputObject
 <Microsoft.Azure.Commands.FrontDoor.Models.PSFrontendEndpoint> [-MinimumTlsVersion <System.String>] [-Confirm]
[-WhatIf] [<CommonParameters>]

Enable-AzFrontDoorCustomDomainHttps [-DefaultProfile

<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -InputObject
 <Microsoft.Azure.Commands.FrontDoor.Models.PSFrontendEndpoint> [-MinimumTlsVersion <System.String>]
-SecretName <System.String> [-SecretVersion <System.String>]
 -VaultId <System.String> [-Confirm] [-WhatIf] [<CommonParameters>]

Enable-AzFrontDoorCustomDomainHttps [-DefaultProfile

<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-MinimumTlsVersion
 <System.String>] -ResourceId <System.String> [-Confirm] [-WhatIf] [<CommonParameters>]

Enable-AzFrontDoorCustomDomainHttps [-DefaultProfile

<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-MinimumTlsVersion
 <System.String>] -ResourceId <System.String> -SecretName <System.String> [-SecretVersion <System.String>] -VaultId
 <System.String> [-Confirm] [-WhatIf]
 [<CommonParameters>]

DESCRIPTION

The Enable-AzFrontDoorCustomDomainHttps enables HTTPS for a custom domain.

PARAMETERS

-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>

The credentials, account, tenant, and subscription used for communication with Azure.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-FrontDoorName <System.String>

The name of the Front Door.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-FrontendEndpointName <System.String>

Frontend endpoint name.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-InputObject <Microsoft.Azure.Commands.FrontDoor.Models.PSFrontendEndpoint>

The Frontend endpoint object to update.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-MinimumTlsVersion <System.String>

The minimum TLS version required from the clients to establish an SSL handshake with Front Door.

Required? false

Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-ResourceGroupName <System.String>

The resource group to which the Front Door belongs.

Required? true
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-ResourceId <System.String>

Resource Id of the Front Door endpoint to enable https

Required? true
Position? named
Default value None
Accept pipeline input? True (ByPropertyName)
Accept wildcard characters? false

-SecretName <System.String>

The name of the Key Vault secret representing the full certificate PFX

Required? true
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-SecretVersion <System.String>

The version of the Key Vault secret representing the full certificate PFX. If not specified, the 'Latest' version will always been used and the deployed

certificate will be automatically rotated to the latest version when a newer version of the certificate is available.

Required? false
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-VaultId <System.String>

The Key Vault id containing the SSL certificate

Required? true
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-Confirm <System.Management.Automation.SwitchParameter>

Prompts you for confirmation before running the cmdlet.

Required? false
Position? named
Default value False
Accept pipeline input? False
Accept wildcard characters? false

-WhatIf <System.Management.Automation.SwitchParameter>

Shows what would happen if the cmdlet runs. The cmdlet is not run.

Required? false
Position? named

Default value False
Accept pipeline input? False
Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, PipelineVariable, and OutVariable. For more information, see about_CommonParameters (<https://go.microsoft.com/fwlink/?LinkID=113216>).

INPUTS

System.String

OUTPUTS

Microsoft.Azure.Commands.FrontDoor.Models.PSFrontendEndpoint

NOTES

Example 1: Enable HTTPS for a custom domain with FrontDoorName and ResourceGroupName using Front Door managed certificate.

```
Enable-AzFrontDoorCustomDomainHttps -ResourceGroupName "resourcegroup1" -FrontDoorName "frontdoor1"  
-FrontendEndpointName "frontendpointname1-custom-xyz"  
-MinimumTlsVersion "1.2"
```

HostName : frontendpointname1.custom.xyz

SessionAffinityEnabledState : Disabled
SessionAffinityTtlSeconds : 0
WebApplicationFirewallPolicyLink :
Backends :
CustomHttpsProvisioningState : Enabling
CustomHttpsProvisioningSubstate : SubmittingDomainControlValidationRequest
CertificateSource : FrontDoor
ProtocolType : ServerNameIndication
MinimumTlsVersion : 1.2
Vault :
SecretName :
SecretVersion :
CertificateType :
ResourceState : Enabled
Id : /subscriptions/{guid}/resourcegroups/resourcegroup1

/providers/Microsoft.Network/frontdoors/frontdoor1/frontendendpoints/frontendpointname1-custom-xyz

Name : frontendpointname1-custom-xyz
Type : Microsoft.Network/frontdoors/frontendendpoints

Enable HTTPS for a custom domain "frontendpointname1-custom-xyz" that is part of Front Door "frontdoor1" in resource group "resourcegroup1" using Front Door managed certificate.

Example 2: Enable HTTPS for a custom domain with FrontDoorName and ResourceGroupName using customer's own certificate in Key Vault with the specific version.

```
$vaultId = (Get-AzKeyVault -VaultName $vaultName).ResourceId
```

```
Enable-AzFrontDoorCustomDomainHttps -ResourceGroupName "resourcegroup1" -FrontDoorName "frontdoor1"  
-FrontendEndpointName "frontendpointname1-custom-xyz" -VaultId  
$vaultId -secretName $secretName -SecretVersion $secretVersion -MinimumTlsVersion "1.0"
```

HostName : frontendpointname1.custom.xyz
SessionAffinityEnabledState : Disabled
SessionAffinityTtlSeconds : 0
WebApplicationFirewallPolicyLink :
Backends :
CustomHttpsProvisioningState : Enabling
CustomHttpsProvisioningSubstate : SubmittingDomainControlValidationRequest
CertificateSource : AzureKeyVault
ProtocolType : ServerNameIndication
MinimumTlsVersion : 1.0
Vault :
SecretName :
SecretVersion :
CertificateType :
ResourceState : Enabled
Id : /subscriptions/{guid}/resourcegroups/resourcegroup1

/providers/Microsoft.Network/frontdoors/frontdoor1/frontendendpoints/frontendpointname1-custom-xyz

Name : frontendpointname1-custom-xyz
Type : Microsoft.Network/frontdoors/frontendendpoints

Enable HTTPS for a custom domain "frontendpointname1-custom-xyz" that is part of Front Door "frontdoor1" in resource group "resourcegroup1" using customer's own certificate in Key Vault with the specific version.

Example 3: Enable HTTPS for a custom domain with PSFrontendEndpoint object using Front Door managed certificate.

```
Get-AzFrontDoorFrontendEndpoint -ResourceGroupName "resourcegroup1" -FrontDoorName "frontdoor1" -Name "frontendpointname1-custom-xyz" |  
Enable-AzFrontDoorCustomDomainHttps
```

HostName : frontendpointname1.custom.xyz

SessionAffinityEnabledState : Disabled
SessionAffinityTtlSeconds : 0
WebApplicationFirewallPolicyLink :
Backends :
CustomHttpsProvisioningState : Enabling
CustomHttpsProvisioningSubstate : SubmittingDomainControlValidationRequest
CertificateSource : FrontDoor
ProtocolType : ServerNameIndication
MinimumTlsVersion : 1.2
Vault :
SecretName :
SecretVersion :
CertificateType :
ResourceState : Enabled
Id : /subscriptions/{guid}/resourcegroups/resourcegroup1

/providers/Microsoft.Network/frontdoors/frontdoor1/frontendendpoints/frontendpointname1-custom-xyz

Name : frontendpointname1-custom-xyz
Type : Microsoft.Network/frontdoors/frontendendpoints

Enable HTTPS for a custom domain with PSFrontendEndpoint object using Front Door managed certificate.

Example 4: Enable HTTPS for a custom domain with resource id using Front Door managed certificate.

Enable-AzFrontDoorCustomDomainHttps -ResourceId \$resourceId

HostName : frontendpointname1.custom.xyz
SessionAffinityEnabledState : Disabled
SessionAffinityTtlSeconds : 0
WebApplicationFirewallPolicyLink :
Backends :
CustomHttpsProvisioningState : Enabling

CustomHttpsProvisioningSubstate : SubmittingDomainControlValidationRequest

CertificateSource : FrontDoor

ProtocolType : ServerNameIndication

MinimumTlsVersion : 1.2

Vault :

SecretName :

SecretVersion :

CertificateType :

ResourceState : Enabled

Id : /subscriptions/{guid}/resourcegroups/resourcegroup1

/providers/Microsoft.Network/frontdoors/frontdoor1/frontendendpoints/frontendpointname1-custom-xyz

Name : frontendpointname1-custom-xyz

Type : Microsoft.Network/frontdoors/frontendendpoints

Enable HTTPS for a custom domain "frontendpointname1-custom-xyz" with resource id \$resourceId using Front Door managed certificate.

Example 5: Enable HTTPS for a custom domain with FrontDoorName and ResourceGroupName using customer's own certificate in Key Vault with the latest version to enable certificate auto-rotation.

\$vaultId = (Get-AzKeyVault -VaultName \$vaultName).ResourceId

Enable-AzFrontDoorCustomDomainHttps -ResourceGroupName "resourcegroup1" -FrontDoorName "frontdoor1"
-FrontendEndpointName "frontendpointname1-custom-xyz" -VaultId

\$vaultId -secretName \$secretName -MinimumTlsVersion "1.0"

HostName : frontendpointname1.custom.xyz

SessionAffinityEnabledState : Disabled

SessionAffinityTtlSeconds : 0

WebApplicationFirewallPolicyLink :

Backends :

CustomHttpsProvisioningState : Enabling
CustomHttpsProvisioningSubstate : SubmittingDomainControlValidationRequest
CertificateSource : AzureKeyVault
ProtocolType : ServerNameIndication
MinimumTlsVersion : 1.0
Vault :
SecretName :
SecretVersion :
CertificateType :
ResourceState : Enabled
Id : /subscriptions/{guid}/resourcegroups/resourcegroup1

/providers/Microsoft.Network/frontdoors/frontdoor1/frontendendpoints/frontendpointname1-custom-xyz

Name : frontendpointname1-custom-xyz
Type : Microsoft.Network/frontdoors/frontendendpoints

Enable HTTPS for a custom domain "frontendpointname1-custom-xyz" that is part of Front Door "frontdoor1" in resource group "resourcegroup1" using customer's own certificate in Key Vault with the latest version to enable certificate auto-rotation.

RELATED LINKS

Online Version: <https://learn.microsoft.com/powershell/module/az.frontdoor/enable-azfrontdoorcustomdomainhttps>