

403 Forbidden or 401 Unauthorized_Storage

1. Tags

cw.Storage-Conn

cw.TSG

Contents

- [Symptoms](#)
- [Cause](#)
 - [Cause 1](#)
 - [Cause 2](#)
 - [Cause 3](#)
 - [Cause 4](#)
- [Resolution](#)
 - [Verify correct credentials](#)
 - [Review Azure Storage Front End logs](#)
 - [Review Azure Storage Firewall configuration](#)
 - [Investigate Resource Instance scenario](#)
- [Case Coding](#)
- [Product Engineering Escalation](#)
- [More Information](#)
- [Need additional help or have feedback?](#)

Symptoms

You receive the following errors when moving or accessing data to a Storage Account using Azure Portal, PowerShell, Storage Explorer, etc.💎:

(403) Forbidden

(401) Unauthorized

HTTP/1.1 403 This request is not authorized to perform this operation.

The remote server returned an error: (403) Forbidden. HTTP Status Code: 403 - HTTP Error Message: This request is not authorized to perform this operation.

Access denied: You don not have access. Looks like you don't have access to this content. To get access, please contact the owner.

Cause

Cause 1

Wrong Storage Account Keys and/or Storage Account name.

Cause 2

SAS expired

Cause 3

Azure Storage Firewall has been configured and customer's IP/subnet has not been granted access.

Cause 4

Azure Storage Account property PublicNetworkAccess is configured to be Disabled, therefore only access through Private Endpoints will be supported. For more information please visit the [PublicNetworkAccess Wiki page](#).

Resolution

Verify correct credentials

- Check the Storage Account key(s) and make sure they are correct.
- Make sure that the Storage Account name is correct, and has not been mistyped. The above error messages can also be seen if the Storage Account name is not correct.
- If you are using SAS, make sure that it is not expired, for more information see Using shared access signatures(SAS).

Review Azure Storage Front End logs

We'll proceed to review the Storage Front End logs for the Blob service in order to dig further regarding the issue faced. Note: The following Table has only errors logged, therefore successful operations won't show here.

1. [Query the Storage Front End \(FE\) logs](#).
2. Review the Storage FE logs. Pay special attention to fields: HttpStatusCode, Status, InternalStatus, MeasurementStatus, userAgent, RequestURL, ClientIP. TIP: You can add a filter to look for HttpStatusCode == 403.
3. Compare the results found with the following scenarios.
4. Issues related to **PublicNetworkAccess** being disabled blocking the request will include the following results:

- **For REST requests** (Azure Blob & Azure Files(REST)):

```
Status: AuthorizationFailure
MeasurementStatus: PublicAccessAuthorizationFailure
InternalStatus: SAServerOtherError / OAuthServerOtherError
```

- **For SMB Requests -DGrep logs (1/2)** (Azure Files(SMB)): DGrep logs will have the following flags. Take note of the ActivityId of a failed request and continue with XDS Logs.

Status: STATUS_ACCESS_DENIED
 MeasurementStatus: N/A
 InternalStatus: ClientOtherError

- **For SMB request - XDS Logs (2/2)** (Azure Files(SMB)):: We'll need to retrieve the Storage Verbose Logs for the failed operation's ActivityId using "XDS Verbose Logs download" option in ASC Resource Explorer. You should be able to find among the logs, lines like the following:

```
Info: XSmbServer.exe: Public network access is disabled. 04/05/2022 00:13:59.436760 - PID: 7048
Error: XSmbServer.exe: Returning Failure hr = 0xc0000022 04/05/2022 00:13:59.436762 - PID: 7048
```



If we confirm issue is related to **PublicNetworkAccessblocking**, customer will need to:

- Configure Private Endpoints to access Storage.
- Or Re-Enable PublicNetworkAccess

For more information please visit the [PublicNetworkAccess Wiki page](#).

5. Issues related to **Azure Storage Firewall** blocking the request may include the following results:

```
Status: AuthorizationFailure
MeasurementStatus: IpAuthorizationFailure
InternalStatus: OAuthIpAuthorizationError / IpAuthorizationError
```


6. If using [Resource Instance](#), please follow [Investigate Resource Instance scenario](#).

7. Check for the [ClientIP](#) property.

1. If the [ClientIP](#) is showing as an [IPv6](#), please review [how to extract Ipv4 address from Ipv6 Service Tunnel](#) and then [Review Azure Storage Firewall configuration](#).
2. If the [ClientIP](#) is showing as a [Public IPv4](#), please proceed to [Review Azure Storage Firewall configuration](#) and whitelist the address, if required.
3. If the [ClientIP](#) is showing as a [Private IPv4](#), unfortunately, it won't be possible to identify where this address is coming from. To narrow down the the possibilities double check which [Supported configuration](#) and which [First Party Service](#) the customer is using.


Review Azure Storage Firewall configuration

1. Open Azure Support Center Resource Explorer.
2. Search/Navigate to the involved Storage Account and select it.
3. Locate the section "[Azure Storage Firewall and Virtual Networks](#)" within the Storage Account details page.
4. Review the "[Allow access from](#)" property.
 1. If the value is "[All networks](#)", Azure Storage Firewall is **disabled**.
 2. If the value is "[Selected Networks](#)", Azure Storage Firewall is **enabled**.
 1. Proceed to review the "[Virtual Network Rules](#)" section.
 2. Verify that the ClientIP belongs to some of the allowed subnets. **Note:** You can get the ClientIP details from the results in [Review Azure Storage Front End logs](#).

3. If the ClientIP is not included in any subnet, notify the customer and work with him if needed to allow the missing Client IP and/or subnet. Further information at [Configure Azure Storage Firewalls and Virtual Networks](#) 

Investigate Resource Instance scenario

1. Double check [Prerequisites](#) are met.
2. Review current [Resource Instance configuration](#).
 1. If the settings of the account is not as expected, please try to set the resource instance rule again. If the settings are still not correct, please follow the [Product Engineering Escalation](#)
3. [Get the Storage Verbose logs](#) using the ActivityId of the failed request.
4. Make sure that the Authentication type is **Bearer** as indicated in the Prerequisites.

1. If it's not **Bearer**, please ask the customer to make the request using OAuth (Azure AD). For additional guidance please review: [Authorize access to data in Azure Storage](#) 

```
Info: XFEHybridBlob.exe: Auth type = 7
06/29/2022 19:43:37.173883 - PID: 134600 TID: 11360 XFE::RestProcessors::RestProcessorBase::CreateAuthenticationContext (RestProcessorBase.cpp:3957)
on Nephos.Blob_IN_155 / cosmosLog_XFEHybridBlob.exe_6280978.bin / 453C7F0F-301E-009B-57F0-8B3724000000 /

Info: XFEHybridBlob.exe: Chose authentication version based on x-ms-version: 2018-03-28
06/29/2022 19:43:37.173889 - PID: 134600 TID: 11360 XFE::RestProcessors::RestVersionParser::ParseAuthenticationVersionFromRequest (RestVersionParser.cpp:224)
on Nephos.Blob_IN_155 / cosmosLog_XFEHybridBlob.exe_6280978.bin / 453C7F0F-301E-009B-57F0-8B3724000000 /

Info: XFEHybridBlob.exe: Authentication type Bearer
06/29/2022 19:43:37.173896 - PID: 134600 TID: 11360 XFE::Authentication::BlobAuthenticationContextFactory::CreateAuthenticationContext (BlobAuthenticationContextFactory.cpp:203)
on Nephos.Blob_IN_155 / cosmosLog_XFEHybridBlob.exe_6280978.bin / 453C7F0F-301E-009B-57F0-8B3724000000 /
```

2. If further assistance is required with AAD/Oauth authentication with Blob, Table or Queue, please engage **PaaS Dev Storage** team.
5. Check if the Resource Instance configured rules match the resource type part of this request.
 1. Check all log entries with ResourceInstanceRule in it.
 2. A result of 0 means that the rule was **not a match**.
 3. A result of 1 means that the rule was a **match**.
6. Check the BypassNetworkRuleState result:


1. A result of 0 indicates that the resource is **NotElegible**, therefore **not eligible for bypass**.
2. A result of 4 indicates that the resource is **ResourceInstance**, therefore **eligible for bypass**.

```
Info: XFEHybridBlob.exe: [ResourceInstanceRule] Try matching resource /subscriptions/.../resourcegroups/.../providers/Microsoft.Logic/workflows/..._logic_app with rule /subscriptions/.../resourcegroups/.../providers/Microsoft.Logic/workflows/..._logic_app with rule /subscriptions/.../resourcegroups/.../providers/Microsoft.Logic/workflows/..._logic_app, result: 0
07/12/2022 03:53:54.847039 - pid: 129164 tid: 119360 @ XFE::OAuth::Native::OAuthManager::TryMatchResourceInstance (oauthmanager.cpp:1114)
on ms-b121prdst06a5nephos.blob_in_55 / cosmosLog_XFEHybridBlob.exe_4930063.bin / D9032027-901E-0037-2EA3-9599AB000000

Info: XFEHybridBlob.exe: [ResourceInstanceRule] Try matching resource /subscriptions/.../resourcegroups/.../providers/Microsoft.Logic/workflows/..._logic_app with rule /subscriptions/.../resourcegroups/.../providers/Microsoft.Logic/workflows/..._logic_app, result: 0
07/12/2022 03:53:54.847041 - pid: 129164 tid: 119360 @ XFE::OAuth::Native::OAuthManager::TryMatchResourceInstance (oauthmanager.cpp:1114)
on ms-b121prdst06a5nephos.blob_in_55 / cosmosLog_XFEHybridBlob.exe_4930063.bin / D9032027-901E-0037-2EA3-9599AB000000


Info: XFEHybridBlob.exe: [ResourceInstanceRule] Try matching resource /subscriptions/.../resourcegroups/.../providers/Microsoft.Logic/workflows/..._logic_app with rule /subscriptions/.../resourcegroups/.../providers/Microsoft.Logic/workflows/..._logic_app, result: 1
07/12/2022 03:53:54.847046 - pid: 129164 tid: 119360 @ XFE::OAuth::Native::OAuthManager::TryMatchResourceInstance (oauthmanager.cpp:1114)
on ms-b121prdst06a5nephos.blob_in_55 / cosmosLog_XFEHybridBlob.exe_4930063.bin / D9032027-901E-0037-2EA3-9599AB000000

Info: XFEHybridBlob.exe: [ResourceInstanceRule] BypassNetworkRulesState: 4
07/12/2022 03:53:54.847047 - pid: 129164 tid: 119360 @ XFE::OAuth::Native::OAuthManager::EvaluateNetworkRules (oauthmanager.cpp:1180)
on ms-b121prdst06a5nephos.blob_in_55 / cosmosLog_XFEHybridBlob.exe_4930063.bin / D9032027-901E-0037-2EA3-9599AB000000
```

7. If rules are not a match, please ask the customer to fix the Resource Instances rule and make sure that the Resource type is supported in the current [Azure Resource instances trusted services](#) .
8. Check if resource has sufficient RBAC Permissions:

1. Check all log entries with RBAC Authorization in it.
2. Review if IsAccessGranted equals **True**.

```
DEBUG: XFEHybridBlob.exe: RBAC authorization: Old=b5a7d726-2a2c-48d9XXXXXX0000000000, Tid=1, 2d7cd011db47, AadTenant=1, 2d7cd011db47, Subsid=1, 2d7974c36666, AccountName=y, ServiceType=BlobService, SasResType=Container, SasPermission=List, RbacPermissionClause=[Blob_Read], IsAccessGranted=True, (Retriable)MissingAuthorizationData=None 07/12/2022 03:53:54.871253 - pid 129164 tid 104564 @ AuthorizeBearerTokenAccessRequest(RbacAuthorizationTokenAccess) on ms-blobdatastore06aephoe.blob_in_55 / commonLog_XFEHybridBlob.exe_1920563.bin / 09032027-901E-0037-2EA3-9999A3000000
```

9. If source resource does not have the required role assignment on the Storage Account, please ask the customer to ensure that the resource identity has [assigned the correct RBAC role assignments](#) .
10. If all above is correct and issue persists, please follow the [Product Engineering Escalation](#).

Case Coding

For issues related to Azure Storage Firewall:

Root cause - Azure Storage\Storage Account Management\Azure Storage Firewalls and Virtual Networks\IP addresses not whitelisted

For invalid Storage Account Key:

Root cause - Azure Storage\Blobs\Authentication & authorization\Account key issues

For invalid/expired SAS:


Root cause - Azure Storage\Blobs\Authentication & authorization\Account SAS issues

For invalid Storage Account name:

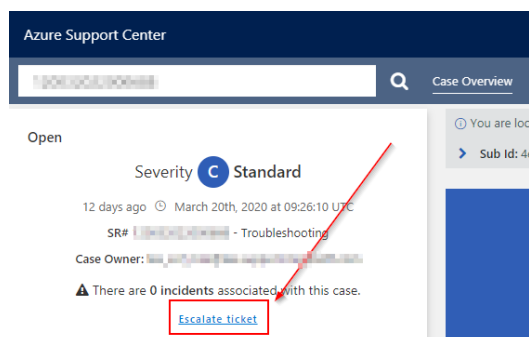
Root cause - Azure Storage\Blobs\Authentication & authorization\Other

Product Engineering Escalation

If you have completed all of the above steps, and are still not able to resolve the issue, you can file an ICM from Azure Support Center(ASC) to get assistance from the engineering team. Please include all relevant troubleshooting information in the ICM.

Note: DO NOT include any PII information in the title of any request. More information can be found [here](#) .



1. You can **file the ICM in Azure Support Center(ASC)** by using the **Escalate ticket** option within **Case Overview** section:



You can create an ICM from within MSSolve.

2. Make sure that the Case has the **correct Support Topic** within the ASC details. If not, please adjust it to the correct one by clicking **Edit & Run Again** in **ASC**.
3. **Select the Template** that best match the Service for the issue, **complete the details required** for the ICM and **submit**.


If you **can't** create the ICM in **Azure Support Center(ASC)**

- For **Severity B and C** issues, you should engage the EEE team, and provide the appropriate template using these links:
 - Storage: <http://aka.ms/cri-xeee> 
- For **Severity A and 0** issues, you should engage WASU, and provide the appropriate template using these links:
 - Storage: <http://aka.ms/CXPCRI-StorageSRP> 

A complete list of all ICM templates is available [here](#) 

More Information

Need additional help or have feedback?

<i>To engage the Azure Storage Connectivity SMEs...</i>	<i>To provide feedback on this page...</i>	<i>To provide kudos on this page...</i>
<p>Please reach out to Azure Storage Connectivity SMEs </p> <p>Make sure to use the Ava process for faster assistance.</p>	<p>Use the Storage Connectivity Feedback form to submit detailed feedback on improvements or new content ideas for Storage Connectivity.</p> <p>Please note the link to the page is required when submitting feedback on existing pages!</p> <p>If it is a new content idea, please put N/A in the Wiki Page Link.</p>	<p>Use the Storage Connectivity Kudos form to submit kudos on the page. Kudos will help us improve our wiki content overall!</p> <p>Please note the link to the page is required when submitting kudos!</p>