Delegate access by using a shared access signature - Azure Storage

By pauljewellmsft

Archived: 2026-04-06 01:27:42 UTC

Important

For optimal security, Microsoft recommends using Microsoft Entra ID with managed identities to authorize requests against blob, queue, and table data, whenever possible. Authorization with Microsoft Entra ID and managed identities provides superior security and ease of use over Shared Key authorization. To learn more, see Authorize with Microsoft Entra ID. To learn more about managed identities, see What are managed identities for Azure resources.

For resources hosted outside of Azure, such as on-premises applications, you can use managed identities through Azure Arc. For example, apps running on Azure Arc-enabled servers can use managed identities to connect to Azure services. To learn more, see Authenticate against Azure resources with Azure Arc-enabled servers.

For scenarios where shared access signatures (SAS) are used, Microsoft recommends using a user delegation SAS. A user delegation SAS is secured with Microsoft Entra credentials instead of the account key. To learn about shared access signatures, see Create a user delegation SAS.

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. You can provide a shared access signature to clients who shouldn't be trusted with your storage account key but who need access to certain storage account resources. By distributing a SAS URI to these clients, you can grant them access to a resource for a specified period of time, with a specified set of permissions.

The URI query parameters that compose the SAS token incorporate all of the information necessary to grant controlled access to a storage resource. A client who has the SAS can make a request against Azure Storage by using just the SAS URI. The information in the SAS token is used to authorize the request.

Azure Storage supports the following types of shared access signatures:

- An account SAS, introduced with version 2015-04-05. This type of SAS delegates access to resources in one or more of the storage services. All of the operations available via a service SAS are also available via an account SAS.

  With the account SAS, you can delegate access to operations that apply to a service, such as `Get/Set Service Properties` and `Get Service Stats`. You can also delegate access to read, write, and delete operations on blob containers, tables, queues, and file shares that are not permitted with a service SAS.

  For more information, see Create an account SAS.

- A service SAS. This type of SAS delegates access to a resource in just one of the storage services: Azure Blob Storage, Azure Queue Storage, Azure Table Storage, or Azure Files. For more information, see Create

a service SAS and Service SAS examples.

- A user delegation SAS, introduced with version 2018-11-09. This type of SAS is secured with Microsoft Entra credentials. It's supported for Blob Storage only, and you can use it to grant access to containers and blobs. For more information, see Create a user delegation SAS.

Additionally, a service SAS can reference a stored access policy that provides another level of control over a set of signatures. This control includes the ability to modify or revoke access to the resource if necessary. For more information, see Define a stored access policy.

Note

Stored access policies are currently not supported for an account SAS or a user delegation SAS.

- Grant limited access to Azure Storage resources by using shared access signatures

---