Recast

Storage Settings

Last Modified on 2026-09-28

Here you can configure the location of the uploaded content items.
You can configure the way Application Workspace Servers access their content on a global scale and you also have the possibility to override the storage settings per server. For more information, see Content Store.

After changing these settings, you will be prompted to reload configurations on all servers. If this step is not completed, the settings will be automatically applied at the next restart. Reloading storage configuration settings does not cause down time on the servers, only invalid configuration parameters cause it.

> Option availability
> This option is visible only for administrators with system levelpermissions. By default, it is visible for the `LOCAL\admin` user, who has system level permissions.

Storage Type

The type of storage the Application Workspace Server will use:

Local

The local storage type will use the `server.json` configuration to access the Content Store.

Azure Blob

Tier – The access tier your blob data has after uploading. New files will always be uploaded as hot, before adjusting to cool if needed.
Authentication method – The authentication method used for accessing the Azure Blob service.

- Shared Key (SK): A storage account wide access key.
- Shared Authentication Signature (SAS): A limited access token that can restrict access to a single container. For more information, see the Microsoft documentation.

Connection string – Only available for the SK authentication method. The connection string can be found in the Azure portal under Storage accounts > your account name > Access keys.
From SAS URI button – Only available for the SAS authentication method. It opens a dialog box where you must insert the SAS generated in Microsoft Azure.
Account URI – Only available for the SAS authentication method. This should contain the URI to the storage account, and not the container's name. For example `https://liquit.blob.core.windows.net/`
Container – The name of the Azure Blob container where all the files are stored.
SAS Query – Only available for the SAS authentication method. The SAS query must start with a question mark (?).

Direct access section

Direct Access options:

- **Disabled** – The direct access functionality for the Azure Blob content is not used, instead the Application Workspace Servers make the content available.
- **Agent** – Agents download content directly from the Azure Blob service by using the query specified in the**Direct Access SAS Query** field.
- **Agentless** – Devices that do not have an Agent running and use Application Workspace through a web browser, download content directly from the Azure Blob service by using the query specified in the **Direct Access SAS Query** field.

- **All** – Devices with or without an Agent running download content directly from the Azure Blob service by using the query specified in the **Direct Access SAS Query** field.

Direct Access authentication method – The following options are available:

- Public access – No tokens are required to access the data.
- Shared Authentication Signature (SAS) – You can access all files with the same token.
- Generate SAS (Requires Shared Key) – A key is generated for each file.

From SAS URI button – It opens a dialog box where you must insert the SAS generated in Microsoft Azure.
Direct Access SAS Query – Used by Agents and web browsers. The SAS query must start with a question mark (?).
Direct Access CDN Endpoint – The URL of the CDN endpoint. Use a CDN that has been configured in front of the Azure Blob services. Content will be distributed globally using a CDN provider. This allows the web browser/agent to download content directly from a server that's near the local device, which improves content distribution times. For more information on how to enable CDN, see Microsoft documentation.

Further reading

How to generate a SAS token