

App Settings Data Storage

Last Modified on 2026-08-07

You can choose to store App Settings data using one of two server-side storage types:

- **Azure Blob** – recommended for fast/global performance; the Application Workspace Agent can have direct access to the content, reducing the load on servers.
- **Network Share** – recommended for on-premises Application Workspace systems; offers complete control over the data.

To configure App Settings storage, navigate to **Manage > System > Storage Settings** and click on the **App Settings** tab.

Azure Blob Storage Options

- **Tier** – The access tier your blob data has after uploading. Files are kept in **Hot** storage because they are volatile, resulting in a lower cost for storing your app settings.
- **Authentication method** – Used for accessing the Azure Blob service.
 - Shared Key (SK): A storage account wide access key.
- **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**.
- **Container** – The name of the Azure Blob container where all the files are stored.
- **Direct Access authentication method** – Available option:
 - Public access – No tokens are required to access the data.
- **Direct Access CDN Endpoint** – The URL of the Azure Content Delivery Network 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 enabling CDN, see [Integrate an Azure Storage account with Azure Content Delivery Network | Microsoft Learn](#)

Network Share Storage Options

- **Path** – network directory where the content is stored; must be accessible by all Application Workspace servers.
- **Credentials** – used by Application Workspace to modify the shared content.

Credentials can be configured under **Manage > Authentication > Credential Store**. We recommend following [Microsoft's guidelines for configuring share and NTFS permissions](#)
