External Resources folder

Last Modified on 05/27/2020 9:59 am EDT

V9.1

Overview

You can set up a shared folder to manage and share all external objects used in workflows, such as JavaScript files, JSON files, CSS files, or images. The shared folder is a virtual directory that can be mapped to the Flowtime or Administration site applications.

Virtual directory name: **ExternalResources**

You run a PowerShell function to set up the virtual directory.

The virtual directory is not overwritten when you redeploy the application.

Supported locations

On premises	Cloud
Network share	Azure Files

Setting up the external resources virtual directory

By default, the external resources folder is mapped to the application's Shared Resources folder.

> **NOTE**
> In Cora SeQuence V9.*x*, each deployed application has its own Shared Resources folder. This folder should be dedicated for application resources only.

To reduce the number of duplicate files and expedite deployment processes, it is recommended that you change the default location to a *centralized location*, and map all site applications to the centralized location.

Prerequisites

Before you set up the ExternalResources virtual directory:

- Create the shared folder in your network or cloud storage service.
- Coordinate with your IT Administrator to make sure that the physical location exists and is accessible to the Application Pool Identity account.

Configuration

1. Run this PowerShell function: Set-CoraSeQuenceExternalResourcesLocation with relevant parameters.
2. Open the ExternalResources folder in the IIS.

Troubleshooting

On opening the ExternalResources folder in the IIS an error is displayed if the Application Pool Identity account user is *NOT* added to the Credential Manager of the server.

Add the user to the Credential Manager by running the below script:

```
cmdkey/add:Azure_File_Share_storage/user:Azure_storage_name/pass:XXXXXXXXXX
```

For example:

```
cmdkey/add:jk.file.core.windows.net/user:joyk/pass:ZHLxxN3I7ZdfpkNDQezMfAiC1A
```

Limitations

Important considerations for setting up the virtual directory.

Location	Requirements
Azure Files and on-premises	The Application Pool Identity account user that will access the virtual directory, needs to: • Have access and permissions to the virtual directory location. • Be a local user on the target server. For details on how to create a local user, see this article. • Be a member of the IIS_USRS group. For more details, see this article.
Azure Files	The Application Pool Identity account user needs to be set as the "Connect As" user.
	For cloud implementations, you can set up the virtual directory on the Azure storage service only.
On-premises	The Application Pool Identity account user that will access the virtual directory, needs to be a domain user.
	The user that connects to the virtual directory from the Administration application needs read/write permissions.
	For on-premises implementations, you can only set up the virtual directory in the same domain.