

CCH Axxess™ Document

Welcome to CCH Axxess Document 2020-3.5

This bulletin provides important information about the 2020-3.5 release of Document. Please review this bulletin carefully. If you have any questions, additional information is available on CCH [Support Online](#).

New in this Release

Document Reports

With this release, a new Export button has been added to the top grid on all reports except the Share Safe audit report. This button allows you to export the report to a CSV file.

Adobe® Acrobat® or Acrobat Reader® 20

Beginning with this release, Document is compatible with Adobe® Acrobat® Standard and Professional 2020.

Security and Performance Feature Updates

Disallowed File Types

By default, Document does not allow certain file types which could present a security risk from being added to Document. The default file types cannot be changed. You can view the list of disallowed file types [here](#).

You can, however, specify additional disallowed file types if needed. You can also prevent specific types of files from being uploaded for particular entity types. This feature reduces the risk that files are uploaded to incorrect entities and can prevent malicious file types from being uploaded to Document.

Allowed Hyperlinks

With this release, to prevent malicious links from being added to Document, you must add a link's URL to the allowed hyperlinks list. Hyperlinks that are not on the allowed hyperlinks list cannot be added to Document.

To add a hyperlink:

1. Open Dashboard, click **Application Links** on the navigation panel, and then click **Lists** under Firm.
2. Click **Document Lists > Allowed Hyperlinks** on the navigation panel.
3. Click **New** on the button bar or click into the first blank row in the grid.
4. Enter the address for the allowed hyperlinks.
5. Press **Enter** on your keyboard.

File List Pagination

Pagination has been added to the Document Central File List tab; the number of files displayed defaults to 500 results. The File List retains your previous pagination from your last logged-in session.

Common Updates

ADSync Tool

If your firm uses the CCH Login (username/password) mode of authentication, the following information is not applicable.

If your firm uses Federated Services with the ADSync Tool, you can now create the OAuth token using a new feature in Dashboard. This new option is only applicable to firms using our Passive with IDaaS mode of authentication. To access this feature, do the following in Dashboard:

1. Click **Application Links**.
2. Click **Utilities** under Firm.
3. Click **Common on the navigation pane**.
4. Click **ADSync Authentication Token**.

Any firm using older modes of Active Directory Integration or ADFS Active mode should continue to use the existing method for AD synchronization.

Firms using the Passive without IDaaS mode of authentication should use the older ADSync Tool or move to Passive with IDaaS to use the newer ADSync Tool.

Please contact our Wolters Kluwer support team if your firm needs to move from Passive without IDaaS to Passive with IDaaS mode of authentication. Click [here](#) for more detail on when and how to use this new OAuth Token for the AD Sync Tool when CCH Access is configured for Passive with IDaaS mode of authentication.