File Analysis Suite

Software Version 3.7.0

Release Notes

Document Release Date: May 2022
Software Release Date: May 2022

Legal notices

Contents

File Analysis Suite Release Notes

Software version: 3.7.0

Publication date: May 2022

This document is an overview of the changes made to File Analysis Suite.

Support matrix

For information about the installation requirements and compatibility with other products, see the File Analysis Suite Support Matrix. The support matrix may be updated between releases so it is available only from the Support portal.

About File Analysis Suite

Micro Focus File Analysis Suite lets you find, protect, and secure sensitive and high-value data within on-premises and cloud unstructured data repositories across your enterprise. Identify, collect, and organize content to ensure discovery of sensitive data. Configure how sources and repositories are processed and categorized with Connect. Analyze your data under management with Analyze. Organize, review, and take action with Manage.

What's new in 3.7.0

The following features and enhancements are included in this release of File Analysis Suite.

General

The following features and enhancements apply to more than one component in File Analysis Suite.

- Added the ability to mask sensitive content based on grammars and entities. The content view visible to the user varies based on whether the user has permission to view the original content that has been masked.

  If the user does not have permission to view content that has been masked:

  - For enriched items, the values of the selected entities are masked from view. Asterisks or a defined string replace the masked characters. Images and PowerPoint slides that have also been OCR'd are not viewable.
  - For items that have not been enriched, the entire item is not viewable. The user is presented with a message stating the items has masked sensitive data and they do not have permission to view the item. Images and PowerPoint slides that have also been OCR'd and contain sensitive data are not viewable.

  If the user has permission to view the content that has been masked:

  - For enriched items, the user has the option to view the masked version with the entity values obfuscated or to view the unmasked version with the entity values visible. When obfuscated, asterisks or a defined string replace the masked characters.
  - For items that have not been enriched, the user sees the text view (not collected) or near-native view (collected) in unmasked view. Without enrichment, the exact entity values are not yet identified.

  If a masking configuration is changed in Connect while a user is viewing documents (in Analyze or Manage) *affected by that change*, the user will not see the masking change on those documents during their current logged in session.

  Data masking is configured on the Manage Grammars page in Connect. A detail panel has been added to let you configure masking quickly and not lose sight of the grammar and entity structure. The masking options presented vary based on the entity being configured. For example, a reference to someone's gender could be not masked, masked entirely, or masked with a defined string and someone's IP address could be not masked, masked entirely, masked with a defined string, or partially masked showing the first or last defined number of characters.

  > **NOTE:** When masking is configured to obfuscate email addresses, masking is not applied to email addresses present in headers.

- Added security permissions for sources and repositories. You can now define the users and groups that have access to specific sources and repositories or choose to not restrict access. When creating a repository, the security permissions are inherited from the source by default. You have the option to further restrict the repository permissions.

  When you restrict a source or repository to only specific users or groups, those users will not be able to view workspaces in Manage that have a data source that includes the repository. Without the permission, the user will see the workspace in the workspace list, but will not be able to open the workspace. When the user attempts to open the workspace, they are presented with a message that they do not have the appropriate permission for the workspace. Users without access to a specific repository will not see items originating from the repository in Analyze > Research or Analyze > Dashboards.
- Added the option to send processed items to a SharePoint target. You can configure SharePoint targets and destinations Connect and send all documents in a workbook to SharePoint targets from Manage.
- Added the option to search for documents based on file size. Using the filter search and search builder in Analyze and Manage to define a file size range (in MB) for items. Items within, and including, the defined range are returned. You can now also create tags based on file size.

  > **NOTE:** File size is defied by positive integers between 0.0 and 999,999 and limited to a single decimal place (`N.n`). The MB file size is converted to bytes and rounded to a whole number. Files with a size up to and including that number of bytes are returned.
- When viewing a protected document in Analyze and Manage, you will see a message in the document view panel that the document has been protected. Previously, when viewing documents in a view that included the document view panel and you selected a protected document, the document view panel was removed from display.
- When exporting documents to a CSV file from Analyze and Manage, you can now include the first and last analyzed dates. These dates represent the first and last date that a document's content was indexed.
- Added the first and last analyzed dates to the Metadata tab of the document detail panel in Analyze and Manage.
- Added sorting by file size to documents lists in Analyze and Manage.

Processing Agent

The following features, enhancements, and important information apply specifically to the processing agent.

- Upgrading the agent from 3.6.x to 3.7.0 does not require uninstalling the 3.6 processing agent. The agent upgrade to 3.7.0 can be performed on top of the 3.6.x agent. For full details, see the File Analysis Suite 3.7.0 Processing Agent Upgrade Technical Note.
- If you are performing the *Custom* installation of the processing agent, do NOT change the SQL"Port or Instance" from the default entry of `1433` when configuring the agent.

  > **CAUTION:** Do not define the instance name or a different port number.

For more information about configuring a named SQL instance to bind to a specific port, see Configure a Server to Listen on a Specific TCP Port on Microsoft Docs.

Connect

The following features and enhancements apply specifically to Connect.

- When editing a repository, added the ability to import the schedule, attribute, and grammar options from a repository template, even if the repository is based on a different template. This action overrides any existing schedule, attribute, or grammar options and can be refined further as needed.
  - To import the schedule from a template, click **LOAD FROM TEMPLATE** on the Schedule page.

    In the resulting dialog, select the desired repository template and then click **OK**. Only the schedule options from the selected template are loaded to the Schedule page and override any options previously selected. Make any additional changes as desired.
  - To import the attributes from a template, click **LOAD FROM TEMPLATE** on the Attributes page.

    In the resulting dialog, select the desired repository template and then click **OK**. Only the attributes from the selected template are loaded to the Attributes page and override any options previously selected. Make any additional changes as desired.
  - To import the grammars from a template, click **LOAD FROM TEMPLATE** on the Grammars Regions page.

    In the resulting dialog, select the desired repository template and then click **OK**. Only the grammars and entities from the selected template are loaded to the Grammar Regions and Grammar Entities pages and override any options previously selected. Make any additional changes as desired.
- Replaced the concept of Custom Connectors for creating sources based solely on IDOL connectors with Custom Adapters. A custom adapter allows you to build a connection between File Analysis Suite and *any* third-party data repository that offers programmatic connection using remote APIs or a client SDK.

  > **NOTE:** Consult File Analysis Suite support for guidance before creating custom adapters. At this time, custom adapters are limited to discovery of items and do not allow for delete actions.
- Added and updated entities.
  - Updated the name entities to now include a title followed by a surname. For example, Mrs. Smith, Dr Smith, Rev Smith, M. Smith, Princess Smith, or Monsieur Smith.
  - Added entity patterns for additional government IDs in multiple languages. These patterns include EHIC Numbers, Healthcare ID Numbers, Pension Numbers, and Unemployment Insurance Numbers.

    - Added medical data entity patterns that include medical terms in multiple languages, as well as blood and laboratory tests, diseases, medical conditions, generic and brand name medical drugs, medical specialties, and surgical procedures in English. US Social Security disability conditions, in English, are also included.
    - Added an entity pattern for VIN numbers (vehicle identification number).
    - Added the phone number pattern for Chile.
- When creating a SharePoint Online source, removed the "Federated Authentication" selection. This selection is no longer necessary for connection.
- Updated the creation of file system and SharePoint repositories to allow you to leave the sub-path entry blank. This results in the repository being *at* the level of the defined source; File Analysis Suite scans the entire source.
- Added a confirmation message when exiting the repository wizard without saving. This verification ensures that you do not unintentionally close the wizard with active unsaved changes.
- Removed the restriction of being able to exclude only specific file types from processing. When creating a repository, you can now type any valid file extension for exclusion from the primary capture rules. This change expands the file types you can exclude from processing.
- On the Agent Activity page, added the ability to cancel a repository update action (task type is *Update*) that has a task status of *Pending*.
- On the Weighted Labels page, added an item count for each weighted label.

Analyze

The following features and enhancements apply specifically to Analyze.

- Updated the Sensitive Data Volume chart in the Analyzed Sensitive Data dashboard and the Total Documents chart in the Data Volume Analysis dashboard to use the date items are indexed instead of the date they are processed. The indexed date reflects when the items were initially analyzed for sensitive data and provides a better reference for when the sensitive data was identified.
- Updated the "Analyzed Content Flagged" chart in the Analyzed Sensitive Data dashboard and the "Content Flagged (Estimated)" chart in the Estimated Sensitive Data dashboard. This chart has been renamed to "Top Weighted Labels" in both dashboards and now shows the top five weighted labels relative to the percentage of overall flagged content. If more than five weighted labels exist, the remaining labels are grouped into an "Other" category on the chart.

Manage

The following features and enhancements apply specifically to Manage.

- Added a permission, *Edit security for all workspaces*, at the application level. When assigned to a role with this permission, the user can set security permissions to any workspace within the

tenant. Due to the broad access of this permission, it is not automatically assigned to any roles.

With this permission, a user can reassign ownership of a workspace if the previous owner leaves the company or is removed as a File Analysis Suite user.

- Added a workspace owner filter to the list of workspaces. You can now show the list of workspaces based on workspace owner. The "Unknown or Deleted Users" option in the filter lets you filter for workspaces assigned to users removed from File Analysis Suite.
- When creating a workspace data source, added the option to filter the available repositories by source. This lets you select the desired source to see only the repositories associated with that source.
- Updated the Workspace Report. If applicable, the workspace due date has been added to the cover of the report and the number of documents protected has been added to the Metrics section.

Administration

Updates to Administration for this release include new permissions discussed in other sections of this Release Notes document.

API updates

The following updates have been made to the File Analysis Suite APIs,

- The prefix on the following API methods has changed from `/cc` to `/analyze`.

Previous API and prefix	3.7.0 API and prefix change
`/cc/v1/data-analytics/overall`	`/analyze/v1/data-analytics/overall`
`/cc/v1/data-analytics/repositories`	`/analyze/v1/data-analytics/repositories`
`/cc/v1/data-analytics/clusters`	`/analyze/v1/data-analytics/clusters`
`/cc/v1/data-analytics/repository-custom-property/{customPropId}`	`/analyze/v1/data-analytics/repository-custom-property/{customPropId}`
`/cc/v1/data-analytics/entities`	`/analyze/v1/data-analytics/entities`
`/cc/v1/data-analytics/sensitive-data-over-time`	`/analyze/v1/data-analytics/sensitive-data-over-time`
`/cc/v1/predicted-data-analytics/overall`	`/analyze/v1/predicted-data-analytics/overall`
`/cc/v1/predicted-data-analytics/repositories`	`/analyze/v1/predicted-data-analytics/repositories`
`/cc/v1/predicted-data-analytics/clusters`	`/analyze/v1/predicted-data-analytics/clusters`
`/cc/v1/predicted-data-analytics/repository-custom-property/{customPropId}`	`/analyze/v1/predicted-data-analytics/repository-custom-property/{customPropId}`
`/cc/v1/tagging-analytics/tags`	`/analyze/v1/tagging-analytics/tags`
`/cc/v1/tagging-analytics/eduction-entities`	`/analyze/v1/tagging-analytics/eduction-entities`
`/cc/v1/tagging-analytics/eduction-entities-timeline`	`/analyze/v1/tagging-analytics/eduction-entities-timeline`

- With the ability to mask data that is processed by File Analysis Suite, changes were required to ensure masked data is not exposed. Several methods have been updated to restrict specific fields from being returned. Additionally, you no longer request an empty set of fields (return all fields) from any method.

  The following methods can no longer be used to request the `CONTENT_PRIMARY`, `EMBEDDED`, `ENTITIES`, or `OCR` metadata fields.

  - `/research/v1/document/{documentId}/metadata`
  - `/research/v1/document/search`
  - `/research/v1/document/token`
  - `/research/v1/document/export-metadata`

- `/ca/v1/workspace/{workspaceId}/document/{documentId}/metadata`
- `/ca/v1/workspace/{workspaceId}/query/document`
- `/ca/v1/workspace/{workspaceId}/query/token`
- `/ca/v1/workspace/document/export-metadata`
- `/ca/v1/workspace/{workspaceId}/workbook/{workbookId}/documents`

  > **NOTE:** If you have the *Manage* > *View masked content* permission you will still be allowed to request the ENTITIES field for this method.

- `/ca/v1/workspace/{workspaceId}/data/reporting-group-partition-map`

To correctly return the `CONTENT_PRIMARY`, `EMBEDDED`, or `OCR` metadata fields, use the `/view/preview-text-content` method.

To correctly return the ENTITIES metadata field, use one of the following methods.

- For Research, in Analyze, use `research/v1/document/{documentId}/privacy-metadata`.
- For Manage, use `/ca/v1/workspace/{workspaceId}/document/{documentId}/privacy-metadata`.

Documentation

File Analysis Suite includes Help Centers that are incorporated into each User Interface and are updated with each software release as appropriate.

To view the File Analysis Suite documentation outside of the product, visit Support & Services on the Micro Focus web site, www.microfocus.com.

To navigate to the File Analysis Suite documentation

1. From the Micro Focus home page click **Support & Services** in the primary menu along the top of the page and then click **Support**.
2. In the Browse Resources section, click **Documentation**.
3. In the product selection list, begin typing **File Analysis Suite**. As you type, products matching what you type display; click **File Analysis Suite**.

   Select the desired release version.

You must have Adobe® Reader installed to view files in PDF format (*.pdf). To download Adobe Reader, go to the Adobe web site.

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Micro Focus File Analysis Suite 3.7.0 Release Notes

Add your feedback to the email and click **Send**.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to FAS.docFeedback@microfocus.com.

We appreciate your feedback!